IBM Storage Protect for Cloud

User Guide

Contents

Note:

Before you use this information and the product it supports, read the information in "Notices" on page 131.

Edition Notice (June 2024)

This edition applies to IBM® Storage Protect for Cloud (product number 5900-AP6) all subsequent releases and modifications until otherwise indicated in new editions.

About this publication

This publication provides overview, planning, and user instructions for IBM® Storage Protect for Cloud Salesforce.

Who should read this publication

This publication is intended for administrators and users who are responsible for implementing a backup and data restore solution using IBM® Storage Protect for Cloud Salesforce. Users can find procedures on how to configure backup, restore, and view job reports for Salesforce organization.

What's new

Learn about new features and updates in IBM® Storage Protect for Cloud Salesforce.

Release Date: January18th, 2026

New features and updates

- IBM® Storage Protect for Cloud Salesforce now provides Public APIs that allow you to retrieve:
  - Job details
  - Basic details of unusual activities
  - Basic information of data alert
- Sandbox seeding now supports condition groups with both **And** and **Or** relationships when editing selected objects in the data scope.
- When restoring data in IBM® Storage Protect for Cloud Salesforce, you can individually deactivate related triggers, workflow rules, flows and processes, or validation rules during the restore.
- When you download exported data from the **Job monitor** > **Job details** page, files exceeding 50 GB will be divided into multiple smaller files. You can then download each of these files individually.

About IBM® Storage Protect for Cloud Salesforce

IBM® Storage Protect for Cloud Salesforce provides a comprehensive backup and restore solution for Salesforce. Our cloud-hosted solution allows for a quick restore of Salesforce records, including all attachments and preservation of relationships between data. It also provides an easy fix for securing your Salesforce content with automatic daily backups, on-demand backups, and comprehensive restores.

IBM® Storage Protect for Cloud Salesforce backs up and restores metadata with Salesforce metadata API, record data with SOAP API, and record files with REST API. Any backup that includes more than 2,000 records is a good candidate for Bulk API 2.0 to successfully prepare, execute, and manage an asynchronous workflow using the Bulk framework. Additionally, using Bulk API can help conserve SOAP API resources. For details, refer to Bulk API and Bulk API 2.0 Limits and Allocations.

The Help (?) list in the left navigation contains the user guide and release notes links to help you catch up with what's new and directs you to IBM® Storage Protect for Cloud interface to submit feedback or invite support for assistance.

Supported and Unsupported Object Types

IBM® Storage Protect for Cloud Salesforce cannot currently backup and restore certain Salesforce objects. For information about the unsupported objects, refer to "Appendix B - Supported and Unsupported Objects for Backup and Restore" on page 86.

Supported Browsers

The following table provides the browsers and their versions that support IBM® Storage Protect for Cloud Salesforce service:

Browsers	Versions
Google Chrome	The latest version
Mozilla Firefox	The latest version
Safari	The latest version
Microsoft Edge based on Chromium	The latest version

Supported and Unsupported Object Types

For information about the objects that can be backed up and restored by IBM® Storage Protect for Cloud Salesforce, refer to "Appendix B - Supported and Unsupported Objects for Backup and Restore" on page 86.

Supported Browsers

The following table provides the browsers and their versions that support IBM® Storage Protect for Cloud Salesforce service:

Browser	Version
Google Chrome	The latest version.
Mozilla Firefox	
Safari (Mac OS X)	
Microsoft Edge based on Chromium	

Supported Languages

IBM® Storage Protect for Cloud Salesforce supports the following languages: English, German, and French.

The display language of IBM® Storage Protect for Cloud Salesforce depends on the display language of your browser. If the default language of your browser is not one of the supported languages, the display language will be English.

Supported Salesforce Environments

IBM® Storage Protect for Cloud Salesforce supports the following Salesforce environments:

- Salesforce Commercial
- Salesforce Government Cloud
- Salesforce Government Cloud Plus

> **Note:** We recommend you reach out to your IBM® Storage Protect for Cloud representative to determine which IBM® Storage Protect for Cloud instance is the best fit for your Salesforce environment.

Integration with Microsoft Azure Event Hubs

If you want to build an integration between a hub in Microsoft Azure Event Hubs and the audit records from IBM® Storage Protect for Cloud Salesforce, refer to the instructions in the IBM® Storage Protect for Cloud user guide.

Supported Salesforce Solutions and Applications

IBM® Storage Protect for Cloud Salesforce supports the backup and restore for the following Salesforce solutions in the Salesforce ecosystem:

- B2B Commerce
- Consumer Goods Cloud
- Sales Cloud
- Service Cloud
- Marketing CRM Classic

IBM® Storage Protect for Cloud Salesforce supports the backup and restore for the following Salesforce application in the Salesforce ecosystem:

- CPQ

> **Note:** The configurations of CPQ are not supported.

Subscription Information

Subscription expiration notification emails will be sent to service administrators 10 days before the expiration, 1 day before the expiration, and on the exact expiration date. It will remind service administrators that the account is going to expire, and your data will be maintained for 30 days after the expiration time. You can choose to purchase or renew your subscription to preserve your data and contact IBM Software Support for a copy of the data.

If you want to know which license types in your Salesforce environment will be charged, complete the following steps:

1. Navigate to the Developer Console of Salesforce.
2. In the **Query Editor** tab, execute the following query in the tab:

```
Select name from userlicense where id in(SELECT userlicenseid FROM Profile WHERE
UserType ='Standard') and name !='Chatter Only'
```

The license types that will be charged are displayed in the query result.

IBM® Storage Protect for Cloud Salesforce counts licenses from active Salesforce standard users. If you want to know the number of users in your Salesforce environment that will be charged, complete the following steps:

1. Navigate to the **Query Editor** tab in the Developer Console of Salesforce.
2. Execute the following query in the tab:

   ```
   Select id from UserLicense where name = 'Chatter Only'
   ```

3. If your organization has the Chatter Only license, The ID of the Chatter Only license is displayed in the query result. Copy this ID.
4. If your organization has the Chatter Only license, execute the following query in the tab. Replace **ChatterOnlyId** with the ID you copied above. The number of users that will be charged is displayed in the query result.

   ```
   Select Count(Id) FROM User WHERE IsActive = true and Profile.UserType in ('Standard')
   and Profile.UserLicenseId != 'ChatterOnlyId'
   ```

   If your organization does not have the Chatter Only license and there is no query result in step “3” on page 10 above, execute the following query in the tab. The number of users that will be charged is displayed in the query result.

   ```
   Select Count(Id) FROM User WHERE IsActive = true and Profile.UserType in ('Standard')
   ```

Data Encryption Methods

Data encryption can be divided into two scenarios: data transmission (data in transit) encryption and data storage (data at rest) encryption.

For data transmission encryption, IBM® Storage Protect for Cloud Salesforce is deployed on the Microsoft Azure framework to make outbound Salesforce API calls and internal communications over HTTPS/TLS encrypted channels. Certificate-based authentication is used for internal communications.

For data storage encryption, IBM® Storage Protect for Cloud Salesforce encrypts all the Salesforce data obtained by calling Salesforce APIs with AES 256 using keys unique to each tenant (either default keys or BYOK). The encryption happens before the data is transmitted to storage.

When transmitting the encrypted data to storage, the data transmission encryption will leverage their own data transmission encryption algorithm or protocols applied of the target storage’s available protocols.

FAQs

How can I configure job notifications?

Go to **Settings** › **Notification settings**. Create or edit the notification profile to configure the users/groups that will receive notifications for different job types and statuses.

Can I get notified when there are unusual changes in Salesforce data?

Yes. IBM® Storage Protect for Cloud Salesforce provides the Monitor alerts feature to help you monitor the data changes between backups. Administrators can configure the data alert rules. For example, when there are 100 deleted records in the backup job compared with the last backup, email alerts will be sent. Refer to “Monitor Alerts” on page 70 for details.

Can I run more than one scheduled incremental backup per day?

Yes. You can run four scheduled incremental backup jobs at most within 24 hours, and you can configure the number of jobs and the start time of the first backup job in the backup settings of an organization. The rest of the jobs will automatically run based on your settings.

What types of record relationships can be backed up and restored?

IBM® Storage Protect for Cloud Salesforce supports the backup and restoration of Lookup Relationships, Hierarchical Relationships, Master-Detail Relationships, Many-to-Many Relationships, and Circular Relationships.

.

Can attachments be restored?

Yes. The attachments can be restored together with records. You can also select to restore the **Attachment** object in the restore jobs.

Is Salesforce Lighting platform supported?

Yes. IBM® Storage Protect for Cloud Salesforce supports the backup and restore of the data in the Salesforce Lightning platform.

Is Salesforce Finiancial Services Cloud platform supported?

Yes. IBM® Storage Protect for Cloud Salesforce supports the backup and restore of the data in the Salesforce Financial Services Cloud platform. For detailed supported and unsupported objects, refer to *Supported and Unsupported Salesforce Financial Services Cloud Objects* in IBM Documentation.

What about the support status of third-party apps?

There will be three types of data after a third-party app is installed:

- Installed package – This data cannot be backed up or restored byIBM® Storage Protect for Cloud Salesforce.
- Configurations (settings/metadata) – This data cannot be backed up or restored by IBM® Storage Protect for Cloud Salesforce.
- Custom objects – Some of the apps allow users to create objects in Salesforce, and users can create records under the objects. IBM® Storage Protect for Cloud Salesforce can back up and restore these custom objects generated by third-party apps.

Get Started

To do list to start using IBM® Storage Protect for Cloud Salesforce.

Refer to the following steps to get started with IBM® Storage Protect for Cloud Salesforce:

1. **Obtain a Subscription**
   - To get a free trial of IBM® Storage Protect for Cloud Salesforce, visit Start your 30-day trial.
   - IBM® Storage Protect for Cloud Salesforce counts licenses from Salesforce users with specific license types. For more details, refer to Subscription Information.
2. **Access IBM® Storage Protect for Cloud**
   "Register for IBM Storage Protect for Cloud Salesforce Account" on page 13 and then register for a Salesforce Backup account in IBM® Storage Protect for Cloud.
3. **Connect your Organization**
   To protect your Salesforce organization via IBM® Storage Protect for Cloud, first connect the organization to IBM® Storage Protect for Cloud. For details, refer to Connect your Tenants to IBM® Storage Protect for Cloud.

   > **Note:** Ensure that the registered user of your Salesforce organization has the **API Enabled** administrative permission assigned in Salesforce Lightning by navigating to **Setup** > **Users** > **Profiles**. This API feature is enabled by default for Performance, Unlimited, Enterprise, and Developer Editions. Some Professional Edition organizations have the API enabled. If it is not enabled in your organization, you may need to contact IBM Software Support for assistance.
4. **Configure the Service App Profile**
   In IBM® Storage Protect for Cloud, create a IBM® Storage Protect for Cloud Salesforce app profile for the tenant. For details, refer to the Create an App Profile.
5. **Configure Backup Scope and Frequency**
   Navigate to IBM® Storage Protect for Cloud Salesforce > **Backup**. Click the More commands (•••) button in the upper-right corner of the organization tile, and then click **Configure backup settings** from the drop-down list. For details, refer to Configure Backup Settings.
6. **Monitor and Manage Backups**
   - To configure additional backup settings such as organization management, user management, storage configuration, notifications, API usage, data retention, encryption, and anonymization, refer to Configure Settings.
   - Regularly monitor the backup status and ensure that backups are running as scheduled. For details, refer to Monitor and Manage Your Backup.
   - Use the reports to monitor your subscription, API usage, and activities in IBM® Storage Protect for Cloud Salesforce, and any unusual activities in your Salesforce environment. The following reports are provided:
     - Subscription Consumption Report
     - API Usage Report
     - User Activities
     - Salesforce Unusual Activities Analysis Report
   - To run Compare jobs to compare data between two different backups or between a backup and the current Salesforce environment, refer to Compare Backup Data.
   - To run a global full-text search to efficiently find what you need and take action to the Discover results, refer to Discover Backup Data.
7. **Perform the Restore**
   - To restore and export backup data from the IBM® Storage Protect for Cloud Salesforce interface, refer to Restore Backup Data.

8. **Perform Sandbox Seeding**
   To create templates and run sandbox seeding jobs to seed the backup data to your sandbox organization, refer to Perform Sandbox Seeding.

Register for IBM® Storage Protect for Cloud Salesforce Account

IBM® Storage Protect for Cloud Salesforce is integrated with IBM® Storage Protect for Cloud. To use IBM® Storage Protect for Cloud Salesforce in IBM® Storage Protect for Cloud, you must first register have an account. Follow the links below:

- Request a trial of IBM® Storage Protect for Cloud Salesforce.
- Contact IBM Sales.

There is a predefined **Administrators** group in IBM® Storage Protect for Cloud Salesforce, which automatically includes the following users defined in IBM® Storage Protect for Cloud:

- Service Administrators (including the tenant owner)
- Application Administrators

Users in the **Administrators** group have full control permission to IBM® Storage Protect for Cloud Salesforce, which means they can use all of the features of IBM® Storage Protect for Cloud Salesforce.

In IBM® Storage Protect for Cloud Salesforce, you can navigate back to the IBM® Storage Protect for Cloud home page. Click the **Other online services** (⠿) button in the upper-right corner of the IBM® Storage Protect for Cloud Salesforce interface. A navigation list appears. You can click **IBM® Storage Protect for Cloud** in the navigation list to go back to the **IBM® Storage Protect for Cloud** interface, or you can also click on other products to access the corresponding products that you have subscriptions.

Create an App Profile

Once a Salesforce organization has been successfully connected, create a IBM® Storage Protect for Cloud Salesforce app profile for the organization. For details, refer to Create an App Profile in the IBM® Storage Protect for Cloud user guide.

Required Permissions:

- To back up and restore your data using IBM® Storage Protect for Cloud, make sure the account that connect the Salesforce organization in IBM® Storage Protect for Cloud has the **API Enabled**, **Manage Users**, and **Modify Metadata Through Metadata API Functions/Modify All Data** system permissions. To back up data, make sure the account also has the **Read** permission to all parent object records of the data you want to back up. To back up all files in the environment, make sure the account also has the **Query All Files** permission. To restore data, make sure the account also has the **Edit** and **Create** permissions to all parent object records of the data you want to restore.
- To back up field values, make sure the account that connect the Salesforce organization in IBM® Storage Protect for Cloud has the **Read** permission to the fields you want to protect.
- To back up objects, make sure the account that connect the Salesforce organization in IBM® Storage Protect for Cloud has the **Read** permission to the objects you want to protect.
- To backup records of user activities, make sure the account that connects the Salesforce organization in IBM® Storage Protect for Cloud has the **View All Data** permission.
- To restore the audit fields, including **CreateById** and **CreatedDate** fields, enable the **Set Audit Fields upon Record Creation** and **Update Records with Inactive Owners** permissions in Salesforce.

To check the permissions of the authenticated user for the organization connection, refer to Back Up Data.

If the connected user does not have sufficient permissions, you need to re-authorize the app profile by following the instructions in Re-authorize an App Profile.

Salesforce Full Restore Best Practices

IBM® Storage Protect for Cloud Salesforce provides a comprehensive solution for Salesforce to assist you to perform the full restore of your organizations.

To make sure the restore jobs can be run successfully, refer to the instructions below to see how to prepare the destination Salesforce environments and configure the restore settings for the restore jobs.

Prepare Your Destination Environments

About this task

Refer to the illustrations below to prepare your destination environments before the full restore:

Procedure

1. Make sure the storage size of the destination organization is sufficient. The storage size of the destination environment should be greater than that of the source environment.
   To check the size of the destination Salesforce environment, go to Salesforce > **Setup** > **Administer** > **Data Management** > **Storage Usage**.
2. Make sure the API count of the destination environment is sufficient, and it depends on the number of records that will be restored:
   - If you restore records only, 3 APIs are required for every 200 records.
   - If you restore records together with attachments, 5 APIs or more are required for every 200 records.

     > **Note:** The restore job may consume more APIs if the total attachment size is large.

     To check the API count of the destination Salesforce environment, go to Classic Salesforce > **Setup** > **Administer** > **Company Profile** > **Company Information**.
3. If you are about to restore your data to another organization, restore the metadata first to keep the metadata of the two environments consistent.
4. If you are about to restore your data to another organization, make sure you have configured a user mapping properly. You can set the Administrator of the destination organization as the Default User in your user mapping, and then users without mappings configured will be automatically mapped to the Default User.
5. If end users are using a destination environment, to avoid affecting end user's usage, configure the API limit of the destination environment since restoring mass data may consume a large number of APIs. The default value is 80%. If the destination environment is not used by users temporarily, it can be configured to a higher value, such as 90%.
6. If you have your own custom objects in your source organization, run a Restore Metadata job to restore the **Custom Object** metadata before the full restore.
7. If the number of records that you want to restore is greater than 8 million, for your best experience, contact IBM Software Support for assistance before running the restore jobs.

Run Restore Jobs in IBM® Storage Protect for Cloud Salesforce

About this task

This section provides instructions on how to configure settings and run the restore jobs.

Procedure

1. Click **Restore** in the left navigation.

2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.
3. Select the **Restore data** tile and select **Organization** from the **Level** drop-down list.
4. Click **Next** to configure the data scope.
5. In the **Recovery point** field, select the time from which you want to restore the data and click **Apply**.
6. Click **Next** to configure the restore settings.
7. In the **Where do you want to restore the data?** field, configure the following settings:
    - In-place restore (restore data to the original organization) – In the **Select a default user for restoring records that belong to de-activated users** text box, enter a keyword to load valid users and select a default user.

      > **Note:** The default user must have the **Modify All Data** permission to the specific objects.

    - Out-of-place restore (restore data to another organization) – Select the **Restore the data to another organization** option. Then, select a destination organization from the drop-down list. Select a user mapping profile from the **Which user mapping profile do you want to apply** drop-down list. You can click **View details** next to the drop-down list to view the details of the user mapping profile.

      You can also click **Create new** in the drop-down list to go to the user mapping page and create a new user mapping profile. For details about user mapping, refer to User Mapping.

      Then select the accuracy for restoring records:

        - **Standard precision** can accelerate your restore progress. Using this mode, if you are about to run multiple restore jobs of the same content, there may be duplicate records. If your restore is for single-use or an urgent request, we recommend that you select this mode.
        - If you plan on running the restore more than once, we recommend that you select the **High precision**.
8. Configure detailed settings for the restore job.
   Do you want to skip restoring the *Share records? – Select if you want to skip restoring the *Share (e.g. **AccountShare; CaseShare**) records.

   *Share records are related to the main records only for recording the relationships between records and the shared users. Normally, users cannot view these records in Salesforce. If you are facing data loss, want to restore the data as soon as possible, and do not care about the sharing relationships, you can skip restoring these records to save your restore time

    - **How would you like to handle conflicts of restoring existing records?**
        - If you encounter mass data loss, while you can make sure the data in the destination organization is correctand there is no need to change them, select **Do not overwrite**. This can save the restore time.
        - If you encounter malicious data corruption and have no idea if the data is reliable, select **Overwrite**. It may slow down the restore job, but it is worth taking more time to ensure that your data is accurate.
    - **Deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore** – Turn on the toggle.
      In Salesforce, there may be some automations (triggers, flows, workflow rules, processes, and validation rules) that you do not want to trigger, or some automations may block the restore process. To save the restore time, you can turn on the toggle to temporarily disable the related automations. At the end of the restore jobs, IBM® Storage Protect for Cloud Salesforce will automatically activate them.
    - **Restore audit fields** – If you need to restore **CreateById** and **CreatedDate** fields, turn on the toggle.
    - **Anonymize data in the restore based on the anonymization profile** – Turn off the toggle.
      If you anonymize the data in the restore, the restored data will be anonymized according to your configured template. This setting is designed for building sandboxes with high fidelity fake data.

You do not need to use it for the full restore. For the details about data anonymization, refer to Configure Data Anonymization Profiles.

9. Click **Next** to go to the **Overview** page to view the settings of the restore job.
   Click **Restore** to restore the organization data as your configurations. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

Back Up a Salesforce Organization

IBM® Storage Protect for Cloud Salesforce supports backing up data and audit logs. For details, refer to Back Up Data and Back Up Audit Logs.

Back Up Data

IBM® Storage Protect for Cloud Salesforce service will automatically back up all your Salesforce records at 00:00 local time after your first login and perform one backup job every day. The backup files/attachments will be encrypted and stored in an Azure BLOB Storage, while other backup data will be encrypted and stored on an Azure Database.

When you first perform a backup job for an organization, a backup cycle is started. The backup cycle is one year. The first backup job in one cycle is a full job, and subsequent backup jobs only back up the changed data since the last job. Incremental backup jobs will continue to run during a full backup, giving you more comprehensive protection of your Salesforce environment.

On the **Backup** page, you can view all organizations. Each organization has a separate tile displaying the last backup job status and the next backup job start time.

The **Backup** page will be automatically refreshed every 10 minutes and each time you navigate back to the **Backup** page. You can also click the Refresh (⟳) button to manually retrieve the latest backup status for the organizations.

You can also perform the following actions to manage the backup for organizations:

- After your first login, you can click the More commands (•••) button in the upper-right corner of the organization tile, click **Back up now** from the drop-down list, and select **All objects** in the panel to back up the entire organization for the first time or let IBM® Storage Protect for Cloud Salesforce perform the first backup job automatically at 00:00 local time. You can also select custom backup scope and select the required object in the **Back up now** panel to run an on-demand backup job. Note that the job will not start if there is already a running job for the organization.

  > **Note:** You can only run on-demand backup jobs for specific objects after a full backup.

- The **Back up now** button is only available to administrators and the user groups that have the **Back up now** permission. If the storage location has not been configured for the organization, the alert will appear. You can select to configure the storage location immediately or configure it later. To configure the storage location, refer to "Configure a Custom Storage Location and Database" on page 46 for instructions.

- The scheduled permission check for the authenticated user will be enabled by default. To disable scheduled permission check or configure permission check settings, click the More commands (•••) button in the upper-right corner of the organization tile and select **Configure permission check settings**. You can configure the following settings:

  - **Start time** – Select the start time of the schedule, and the first permission check will be automatically performed at that start time. By default, the start time is the date when the Salesforce organization is connected.

  - **Interval** – Configure the interval for the scheduled permission check. By default, the interval is 1 month.

- To perform an immediate permission check, click the More commands (•••) button in the upper-right corner of the organization tile and select **Check Permissions now**. The permission report will be sent to administrators.
  The following three lists will be included in the permission report. For the lack of permissions, you can grant the required permissions to the authenticated user and contact IBM support to perform a full backup for the unprotected objects.

  - **FieldPermission**: This list shows whether the authenticated user has the **Read** permission for each field. The **Field Permission** column displays both the field name and the name of the object it belongs to. Note that the field values that are not granted the **Read** permission to the authenticated user cannot be protected.

  - **ObjectPermission**: The objects that are not granted the **Read** permission for the authenticated user will not be included in this list and they cannot be protected. You can check whether the objects you want to protect are specified in this list.
  - **UserPermission**: This list shows the permissions required by the authenticated user for backup and restore. You can check whether each permission has been granted to the authenticated user. Additionally, you can find information on the intended use of any permissions that have not been assigned.

- Administrators can configure the backup scope and frequency for the automatic backups. Click the More (•••) commands button in the upper-right corner of the organization tile and click **Configure backup settings** from the drop-down list. For detailed instructions, refer to “Configure Backup Settings” on page 18.
- When you manage many organizations, and you want to hide specific organization cards from the **Backup** page, click the More commands (•••) button in the upper-right corner of the organization tile and click **Hide organization** from the drop-down list. The organization will be moved to the **Hidden organizations** section. You can then click **Hide** in the upper-right corner to hide the organization cards.
  If you want to view the hidden organizations, click **Show hidden organizations**. If you want to always show an organization, click the More commands (•••) button in the upper-right corner of the organization tile and click **Show organization** from the drop-down list.
- You can check the backup details of an organization by clicking on the corresponding organization tile. You can also click the More actions (•••) button in the upper-right corner of the organization tile and click **View details** from the drop-down list to view the backup details. For details, refer to “Monitor and Manage Your Backup” on page 19.

Note the following about backup:

- To protect all files of an organization, the user who creates the Salesforce app profile must have the Query All Files permission. For details on connecting Salesforce organization, refer to Connect your tenants to IBM Storage Protect for Cloud.
- Once your subscription expires, the backup schedule will be stopped.
- The backup jobs will back up the objects with exceptions in the last backup job automatically.
- Within 24 hours, you can perform different numbers of backup jobs for organizations with different subscription types. Refer to “Appendix D - IBM Storage Protect for Cloud Salesforce Subscription Retention Information” on page 125 for details. Skipped and failed jobs are not included in the limitation on the number of jobs.
- If IBM® Storage Protect for Cloud Salesforce Services detects that the number of your active users in Salesforce has exceeded the number of purchased user seats for IBM® Storage Protect for Cloud Salesforce, IBM® Storage Protect for Cloud Salesforce will stop the backup feature. You can still restore or compare data using the previous backups.
  The number of Sandbox users will not be counted as active users in Salesforce.

Configure Backup Settings

To configure backup settings for data backup, click the More commands (•••) button in the upper-right corner of the organization tile on the **Backup** page, and then click **Configure backup settings** from the drop-down list. If you have audit log backup enabled for the organization, select **Data backup**. Then you can turn on/off the toggle next to the organization name to enable/disable the data backup for the organization. Once the backup is enabled, you can configure the backup scope and backup frequency of the organization.

> **Note:** If a backup job is already running for the organization, the scheduled backup job will be automatically skipped.

Configure the Backup Scope

Procedure

To configure the backup scope, complete the following steps:

1. In the **Backup scope** tab, turn on/off the toggles to configure if you want to back up the *Feed (for example: **Account Feed**; **Contact Feed**; **Case Feed**) and *Share (for example: **Account Share**; **Contact Share**; **Case Share**) objects of the organization. Note that if you back up these objects, the backup performance may be affected, and they will take up extra storage space.
2. Turn on/off the toggle to configure if you want to back up event logs. After turning on the toggle, you can select to back up **Daily event logs** or **Hourly event logs**.
3. Turn on the toggle to **Exclude specific object types from backup** and select the objects you do not want to protect from the **Objects** drop-down list.
4. Turn on the toggle to **Exclude specific metadata types from backup** and select the metadata types you do not want to protect from the **Metadata type** drop-down list.
5. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving any changes.

Configure the Backup Frequency

Procedure

To configure the backup frequency, complete the following steps:

1. In the **Frequency** section under the **Backup data** tab, select a number from the **How many backup jobs would you like to run per day?** drop-down list. IBM® Storage Protect for Cloud Salesforce will automatically provide the job schedule according to the frequency you selected.
   You can change the start time for the first backup job. The rest of the schedules will be automatically calculated and displayed.
2. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving any changes.
   You can change the start time for the first backup job. The rest of the schedules will be automatically calculated and displayed.

Monitor and Manage Your Backup

About this task

You can click an organization’s tile on the **Backup** page to view the data backup details of that organization. If you have audit log backup enabled for the organization, select the **Data backup** tab.

On the **Organization details** page, you can get the time for the **Next incremental backup** and **Next full backup** of the organization data. You can also switch to the desired backup job on the left, download job report, export data, download metadata, or perform a compare job to get the details of the deleted, changed, or added records. For backup jobs in progress, successful items and items with exceptions during the backup are provided.

You can also click the More (•••) commands button on the upper-right corner and select to manually start a backup job for this organization or configure the backup settings

Procedure

For details, refer to the following:

- Click a backup time in the left pane, the details of the corresponding backup job will be displayed in the right pane. You can view the start time, end time, number of records, number of metadata items, and backup size of the job. Click **Download report** to download the job report to XLS file. We are implementing error codes into job reports as a self-service approach for troubleshooting. Clicking the error code link in the downloaded job report will open the“Troubleshooting Guide” on page 76 .
- **Data** – Under this tab, you can view, export, download, and compare the backup data.
  - View the number of records and backup details about different objects. You can click **Filters** to filter the objects by object type or number range of removed/changed/added records.
  - You can **Export records** or **Export files** of the protected objects.

    - To export records, select the objects that you want to export and click **Export records**. In the **Export records** panel, select whether to export detailed backup data to CSV files or MySQL files, and whether you want to export the changed data after the last backup job or export all backup data in the current cycle. Then click **Export**. an export job will be added to the job queue, and you can view the progress of the job in the job monitor.

      To export files, click **Export files** directly. In the **Export files** window, select the objects for which you would like to export files, and whether you want to export the changed data after the last backup job or export all backup data in the current cycle, and then click **Export**. Only the following object types are supported: **Attachment**, **Document**, **Static Resource**, **Mail Merge Template**, and **Content Version**.

      > **Note:** You cannot start an export job when there is an existing export job running. There is a monthly limit (100 GB) on the capacity of files that can be exported.

    - After any export job is completed, two ways are available to download the export data:
        - In **Job monitor**, click the More commands (•••) button of the export job and select **Download data**. Then copy the password and click **Download** to download and save the CSV files or MySQL files to a local location.
        - On the **Job monitor** > **Job details** page, click **Download export data** to download and save the CSV files or MySQL files to a local location. To obtain the password of the downloaded files, click **Show password**.
    - If you want to compare the backup data of the current backup job with those of the latest backup job, click **Compare** link to start a compare job. You can go to Job monitor to follow up the job progress and details.
- **Metadata** – Under this tab, view the backup details of metadata. You can also search for specific metadata by entering the keyword of metadata type in the search box. You can click the **Export metadata** link to export metadata to a ZIP file.

  > **Note:** Several built-in Salesforce profiles do not have the same name when they are exported. If you create a custom profile with the same name as the exported name of the built-in Salesforce profile, the custom profile will overwrite the built-in profile. To avoid overwriting the built-in Salesforce profiles, refer to “Appendix C - Exported Profile Names for Built-in Salesforce Profiles” on page 124 before naming a custom profile.

Back Up Audit Logs

IBM® Storage Protect for Cloud Salesforce now supports the backup and export of Login History, Field History Tracking, and Setup Audit Trail. The feature is currently in private preview. To enable this feature, contact the IBM support team.

Configure Backup Settings

To configure backup settings for audit log backup, click the More commands (•••) button in the upper-right corner of the organization tile on the **Backup** page. Then click **Configure backup settings** from the drop-down list and select **Audit log backup**. You can turn on/off the toggle next to the organization name to enable/disable the audit log backup for the organization. Once the backup is enabled, you can set the start time for the daily audit log backup job. The audit log backup job will then run at the scheduled time every day.

> **Note:** If a backup job is already running for the organization, the scheduled backup job will be automatically skipped.

Monitor and Manage Your Backup

You can click an organization’s tile on the **Backup** page and select the **Audit logbackup** tab to view the audit log backup details of that organization.

On the **Organization details** page, you can get the time for the **Next backup** of audit logs in the organization. You can also switch to the desired backup job on the left, download job report, and export audit logs.

For details, refer to the following:

- Click a backup time in the left pane, and the details of the corresponding backup job will be displayed in the right pane. You can view the start time, end time, number of audit logs, and backup size of the job. Click **Download report** to download the job report to the XLS file.

- To export audit logs that were updated since the last backup jobto CSV files, select the audit logs that you want to export and click **Export audit logs**. Then click **Export** to confirm. An export job will be added to the job queue, and you can view the progress of the job in the job monitor.

  > **Note:** There is a monthly limit (100 GB) on the capacity of audit logs that can be exported.

  After any export job is completed, two ways are available to download the export data:

  - In **Job monitor**, click the More commands (•••) button of the export job and select **Download data**. Then copy the password and click **Download** to download and save the CSV files to a local location.

  - On the **Job monitor** > **Job details** page, click **Download export data** to download and save the CSV files to a local location. To obtain the password of the downloaded files, click **Show password**.

Compare Backup Data

IBM® Storage Protect for Cloud Salesforce provides **Compare data** and **Compare metadata** to compare and show the differences between objects or metadata in two different backups. It can also compare the differences in objects/metadata between a backup and the current Salesforce environment. This feature is available to administrators and the users in the groups that have the **Compare** permission.

Compare Data

Procedure

To compare objects, complete the following steps:

1. Click **Compare** in the left navigation, and then select **Compare data**.
2. On the **Compare data** page, select to compare with the backup data or compare with the current Salesforce data.
    - To compare with backup data, in the left section, select the organization and the old recovery point. In the right section, select the new recovery point. You can only compare backup data in the same organization.
    - To compare with Salesforce data in the current organization, in the left section, select the organization and the old recovery point. In the right section, the current organization is automatically displayed. Note that IBM® Storage Protect for Cloud Salesforce now supports getting the deleted records of the AccountShare object when comparing the backup data with the current Salesforce data.
3. In the **Level** field, select whether you want to compare objects or records.
    - To compare objects, select the objects you want to compare from the in the **Object**drop-down list.
    - To compare records, complete the following steps:
        a. Select the objects you want to compare from the **Object** drop-down list.
        b. In the **Keyword** field, you can select to search for records by **Record name** or **Record ID**. Enter the **Record ID** or keywords of the **Record name** and then click **Search**. The default search condition is to search the backup data within the last backup cycle.
        You can click the link in the Record ID column to view the record details.
        c. Select the records you want to restore from the search results. If you click the checkbox next to the **Record ID** column, all the records that meet your search conditions will be selected.
4. Click **Compare** to start the compare process.
    After the compare job has started, you can go to the job monitor to track the progress. After the job is finished, you can click the Job ID link to the view the compare result. For details, refer to "Job Monitor" on page 65.

Compare Metadata

Procedure

To compare metadata, complete the following steps:

1. Click **Compare** in the left navigation, and then select **Compare metadata**.
2. On the **Compare metadata** page, select to compare with the backup metadata or compare with the current Salesforce metadata.
    - To compare with backup metadata, in the left section, select the old organization and recovery point. In the right section, select the new organization and recovery point you want to compare.
    - To compare with Salesforce data, in the left section, select the old organization and recovery point. In the right section, select the new organization you want to compare.
3. Click **Compare** to start the compare process.

After the compare job has started, you can go to the job monitor to track the progress. After the job is finished, you can click the Job ID link to the view the compare result. For details, refer to "Job Monitor" on page 65.

Discover Data

IBM® Storage Protect for Cloud Salesforce offers global full-text search, enabling precise and comprehensive data discovery to effectively find and restore exactly what you need. You can enter the keywords in record ID, record name, or field value to run a global full-text search of your backup data. Note that the results of the discover job will only be available for 30 days.

Discover Backup Data

To discover backup records, complete the following steps:

1. Click **Discover** in the left navigation.
2. On the **Discover** page, use the properties to search for the backup records. Refer to the steps below:
    a. In the **Keywords** field, enter keywords from the record ID, record name, or field value.

    b. From the **Organization** dropdown list, select the Salesforce organization to search from.

    c. In the **Data source** field, select **Backup**.

    d. Click the Calendar (📅) button in the **Recovery Point** field to select a recovery point. We will search the data from the beginning of the last full backup job to the recovery point.

    e. Turn on/off the toggle to define whether to add *Feed and *Share objects to the **Object** dropdown list. If you select to search from *Feed and *Share objects, the discover job may take a long time.

    f. From the **Object** drop-down list, select the objects you want to search from.
    After selecting the objects, you can click **Advanced field-level filter** to select specific fields for each object to search for keywords and then click **Save**. By default, the search includes all fields for each object.
3. Click **Discover** to start the discover process.

After the discover job has started, you can go to the job monitor to track the progress. After the job is finished, you can click the Job ID link to view the discovery results and take actions to the discovered records. For details, refer to Job Monitor.

Perform a Restore

Refer to the following instructions to Restore Backup Data.

Restore Backup Data

IBM® Storage Protect for Cloud Salesforce provides five flexible scenarios to restore your organization's Salesforce data. Before the actual restore of **Objects** and **Records**, you can run a pre-restore and review job recommendations in the **Job monitor**. This enables you to adjust settings as needed, ensuring a smoother and error-free process.

Select an organization from the organization drop-down menu. Click **Restore** to show the **Restore** tab, and select one of the following actions to start.

- “Restore an Organization” on page 25 – Restore all records of an organization.
- “Restore Objects” on page 28 – Restore every record of selected objects. The pre-restore is supported.
- “Restore Records” on page 31 – Restore specific records only. The pre-restore is supported.
- “Restore Fields” on page 36 – Restore the values of specific fields only.
- “Restore Metadata” on page 37 – Restore the metadata of the organization only.

> **Note:** To restore the custom objects and fields, IBM® Storage Protect for Cloud Salesforce adds the corresponding permissions to the mapped users or the default user while running Out of Place Restore jobs.

If you want to set the External ID of objects within the organization as the unique identifier during the restore process if the corresponding Record ID does not exist in the destination organization, refer to Configure External ID.

Configure External ID

IBM® Storage Protect for Cloud Salesforce supports configuring the External ID of objects within the organization as the unique identifier in the restore process if the corresponding Record ID does not exist in the destination organization. Note that if the External ID field of a record is blank in the backup data, no records will match in the restore, and it will be created in the destination organization.

Complete the following steps to configure the External ID:

1. Navigate to **Settings** >**General**.
2. Click the **External ID** tab. All organizations that you manage are displayed.
3. Turn on the toggle next to the organization you desired, and the **Configure External ID window** appears.
4. Click **Add**.
5. In the **Object** column, select an object from the drop-down list.
6. In the **External ID** column, select an External ID field for the object from the drop-down list.
7. Repeat Steps 4 through Step 6 to add more objects and select External ID fields for them. To delete objects in the table, click the Delete (🗑) icon under the **Action** column.
8. Click **Save** to save the configuration.

Restore an Organization

You can restore an organization to the desired condition by designating the backup job of a specific moment that you want to restore to. The **Restore Organization** option is only available to the user groups that have the

Restore organization permission. For a comprehensive solution for Salesforce to assist you to perform the full restore of your organizations, refer to Salesforce Full Restore Best Practices.

Organization level restores are unavailable for the trial subscription. To restore all data in an organization, you can contact IBM support for assistance.

You can choose one of the following ways to restore all records in an organization:

- "In Place Restore" on page 26 – Restore an organization backup to the original organization.
- "Out of Place Restore" on page 27 – Restore a source organization backup to another organization.

Note that the Restore Organization job (especially out-of-place restore) may be time-consuming.

In Place Restore

Procedure

To restore an organization backup to the original organization, complete the following steps.

1. Click **Restore** in the left navigation.
2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.
3. Select the **Restore data** tile and select **Organization** from the **Level** drop-down list.
4. Click **Next** to configure the data scope.
5. In the **Recovery point** field, select the time from which you want to restore the data and click **Apply**.
6. Click **Next** to configure the restore settings.
7. In the **Configure restore settings** step, configure the following settings:
   - **Where do you want to restore the data?**– Select the **Restore the data to the original organization** option.
   - In the **Select a default user for restoring records that belong to deactivated users** text box, enter a keyword of usernames to load valid users and select a default user.

     > **Note:** The default user must have the **Modify All Data** permission to the specific objects.

   - **Do you want to skip restoring the *Share records?** – Select if you want to skip restoring the *Share (e.g. **AccountShare; CaseShare**) records.
     *Share records are related to the main records only for recording the relationships between records and the shared users. Normally, users cannot view these records in Salesforce. If you are facing data loss, want to restore the data as soon as possible, and do not care about the sharing relationships, you can skip restoring these records to save your restore time
   - **How would you like to handle conflicts of restoring existing records?** – Select **Do not overwrite** if you would like to keep the current record when a conflict occurs; select **Overwrite** if you would like to keep the backup record.
   - **Deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore** – Turn on/off the toggle and select the specific automation types to define if you want to deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore. They will be activated when the restore job is completed.
   - **Restore audit fields** – Turn on/off the toggle to define if you want to restore audit fields, including **CreateById** and **CreatedDate** fields. If you select to restore, IBM® Storage Protect for Cloud Salesforce will restore the fields based on the backup values. If not, the created by user will be the user that has connected the Salesforce organization in IBM® Storage Protect for Cloud; the created time will be the restore time. Only the following object types are supported for audit field restore: **Account**, **Article Version**, **Attachment**, **Campaign Member**, **Case**, **Case Comment**, **Contact**, **Content Version**, **Contract**, **Event**, **Idea**, **Idea Comment**, **Lead**, **Opportunity**, **Question**, **Task**, **Vote**, and custom objects.

> **Note:** To restore the audit fields, enable the **Set Audit Fields upon Record Creation** and **Update Records with Inactive Owners** permissions in Salesforce.

- **Anonymize data in the restore based on the anonymization profile** – Turn on/off the toggle to define if you would like to anonymize the backup data to high fidelity fake data generated by IBM® Storage Protect for Cloud Salesforce and restore it to your organization. When there is no enabled anonymization profile for your organization, you can click the **Settings > Profile management** link to configure one if you are the Administrator, and then click the **Refresh** button to load the profile.

> **Note:** We do not recommend that you anonymize the data and restore it to your production organization since it may bring risks of data corruption.

8. Click **Next** to go to the **Overview** page to view the settings of the restore job.
9. Click **Restore** to restore the organization data as your configurations. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

Out of Place Restore

Before you begin

If you have customized metadata configured in your source Salesforce, the customized metadata cannot be restored to another organization directly. Prior to the restore, make sure the same metadata settings are configured in the destination organization. Also, be sure that the storage space of the destination organization is sufficient for the restore.

Procedure

To restore a source organization backup to another organization, complete the following steps.

1. Click **Restore** in the left navigation.
2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.
3. Select the **Restore data** tile and select **Organization** from the **Level** drop-down list.
4. Click **Next** to configure the data scope.
5. In the **Recovery point** field, select the time from which you want to restore the data and click **Apply**.
6. Click **Next** to configure the restore settings.
7. In the **Configure restore settings** step, configure the following settings:
   - **Where do you want to restore the data?** – Select the **Restore the data to another organization** option. Then, select a destination organization from the drop-down list.
     Select a user mapping profile from the **Which user mapping profile do you want to apply** drop-down list. You can click **View details** next to the drop-down list to view the details of the user mapping profile.

     You can also click **Create new** in the drop-down list to go to the user mapping page and create a new user mapping profile. For details about user mapping, refer to User Mapping.
   - **Select the accuracy for restoring records** – Select to run the restore job in the Standard precision or High precision.
     - **Standard precision** can accelerate your restore progress. Using this mode, if you are about to run multiple restore jobs of the same content, there may be duplicate records. If your restore is for single-use or an urgent request, we recommend that you select this mode.
     - If you plan on running the restore more than once, we recommend that you select the **High precision**.
   - **Do you want to skip restoring the *Share records?** – Select if you want to skip restoring the *Share (e.g. **AccountShare; CaseShare**) records.

*Share records are related to the main records only for recording the relationships between records and the shared users. Normally, users cannot view these records in Salesforce. If you are facing data loss, want to restore the data as soon as possible, and do not care about the sharing relationships, you can skip restoring these records to save your restore time.

- **How would you like to handle conflicts of restoring existing records?** – Select **Do not overwrite** if you would like to keep the current record when a conflict occurs; select **Overwrite** if you would like to keep the backup record.
- **Deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore** – Turn on/off the toggle and select the specific automation types to define if you want to deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore. They will be activated when the restore job is completed.
- **Restore audit fields** – Turn on/off the toggle to define if you want to restore audit fields, including **CreateById** and **CreatedDate** fields. If you select to restore, IBM® Storage Protect for Cloud Salesforce will restore the fields based on the backup values. If not, the created by user will be the user that has connected the Salesforce organization in IBM® Storage Protect for Cloud; the created time will be the restore time. Only the following object types are supported for audit field restore: **Account**, **Article Version**, **Attachment**, **Campaign Member**, **Case**, **Case Comment**, **Contact**, **Content Version**, **Contract**, **Event**, **Idea**, **Idea Comment**, **Lead**, **Opportunity**, **Question**, **Task**, **Vote**, and custom objects.

> **Note:** To restore the audit fields, enable the **Set Audit Fields upon Record Creation** and **Update Records with Inactive Owners** permissions in Salesforce.

- **Anonymize data in the restore based on the anonymization profile** – Turn on/off the toggle to define if you would like to anonymize the backup data to high fidelity fake data generated by IBM® Storage Protect for Cloud Salesforce and restore it to your organization. When there is no enabled anonymization profile for your organization, you can click the **Settings > Profile management** link to configure one if you are the Administrator, and then click the **Refresh** button to load the profile.

> **Note:** We do not recommend that you anonymize the data and restore it to your production organization since it may bring risks of data corruption.

8. Click **Next** to go to the **Overview** page to view the settings of the restore job.
9. Click **Restore** to restore the organization data as your configurations. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

Restore Objects

You can restore the desired objects only by designating objects through recovery point and object. The object restore is only available to the user groups that have the **Restore objects** permission.

Before the actual restore, you can run a pre-restore and review job recommendations in the Job Monitor. This enables you to adjust settings as needed, ensuring a smoother and error-free process.

You can choose one of the following ways to restore the specific objects:

- In Place Restore – Restore specific objects to the original organization.
- Out of Place Restore – Restore specific objects to another organization.

In Place Restore

Procedure

To restore specific objects to the original organization, complete the following steps.

1. Click **Restore** in the left navigation.
2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.

3. Select the **Restore data** tile and select **Object** from the **Level** drop-down list.
4. Click **Next** to configure the data scope.
5. Click **Run Now** to restore the objects that match your configuration, or click **Cancel** to cancel your configuration and go back to the **Restore** tab.
6. From the **Object** drop-down list, select the objects you want to restore and click **Apply**. You can view the number of records in each selected object.
7. Click **Next** to configure the restore settings.
8. In the **Configure related data** step, configure the following settings:
    - **Restore parent and child object records** – Turn on/off the toggle to define if you want to restore parent and child object records. If you turn on the toggle, the objects you selected will be displayed as **Base** objects below. You can click any object to add its parent or child objects. Subsequently, you can also click the parent or child objects to add grandparent or grandchild objects. For the restore, you can add up to 10 levels of parent objects and 10 levels of child objects.
    - **Restore related fields for deleted records** – If the selected records do not exist in the destination organization, turn on/off the toggle to define if you want to restore these records along with the related fields of their existing first-level child object records. Note that this option is unavailable if the **Restore parent and child object records** option is enabled, and selecting it may affect the restore performance.
9. Click **Next** to configure the restore settings.
10. In the **Configure restore settings** step, configure the following settings:
    - **Where do you want to restore the data?** – Select the **Restore the data to the original organization** option.
      In the **Select a default user for restoring records that belong to deactivated users** text box, enter a keyword of usernames to load valid users and select a default user.

      > **Note:** The default user must have the **Modify All Data** permission for the specific objects.

    - **How would you like to handle conflicts of restoring existing records?** – Select **Do not overwrite** if you would like to keep the current record when a conflict occurs; select **Overwrite** if you would like to keep the backup record.
    - **Deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore** – Turn on/off the toggle and select the specific automation types to define if you want to deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore. They will be activated when the restore job is completed.
      You can customize the deactivation scope in job details of a pre-restore job. For detailed instructions, refer to View Job Details.
    - **Restore records in the recycle bin** – Turn on/off the toggle to define if you want to restore the record from the recycle bin if the record with the same ID still exists in the recycle bin. The record ID will be kept after being restored. If you enable this feature, the record ID will be kept after being restored.
    - **Restore audit fields** – Turn on/off the toggle to define if you want to restore audit fields, including **CreateById** and **CreatedDate** fields. If you select to restore, IBM® Storage Protect for Cloud Salesforce will restore the fields based on the backup values. If not, the created by user will be the user that has connected the Salesforce organization in IBM® Storage Protect for Cloud; the created time will be the restore time. Only the following object types are supported for audit field restore: **Account**, **Article Version**, **Attachment**, **Campaign Member**, **Case**, **Case Comment**, **Contact**, **Content Version**, **Contract**, **Event**, **Idea**, **Idea Comment**, **Lead**, **Opportunity**, **Question**, **Task**, **Vote**, and custom objects.

      > **Note:** To restore the audit fields, enable the **Set Audit Fields upon Record Creation** and **Update Records with Inactive Owners** permissions in Salesforce.

- **Anonymize data in the restore based on the anonymization profile** – Turn on/off the toggle to define if you would like to anonymize the backup data to high fidelity fake data generated by IBM® Storage Protect for Cloud Salesforce and restore it to your organization. When there is no enabled anonymization profile for your organization, you can click the **Settings > Profile management** link to configure one if you are the Administrator, and then click the **Refresh** button to load the profile.

> **Note:** We do not recommend that you anonymize the data and restore it to your production organization since it may bring risks of data corruption.

11. Click **Next** to go to the **Overview** page to view the settings of the restore job.
12. Click **Restore**, and the **Restore** window appears. You can take the following actions:
    - **Pre-restore** – A pre-restore job will run according to the configurations before the actual restore. When the job is finished, you can review job recommendations in the Job Monitor. This enables you to adjust settings as needed, ensuring a smoother and error-free process.
    - **Restore** – The restore job will run directly to restore data to the destination organization. After the job has started, you can go to the Job Monitor to view more job details.

Out of Place Restore

Before you begin

If you have customized metadata configured in your source Salesforce, the customized metadata cannot be restored to another organization directly. Prior to the restore, make sure the same metadata settings are configured in the destination organization.

Procedure

To restore specific objects to another organization, complete the following steps.

1. Click **Restore** in the left navigation.
2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.
3. Select the **Restore data** tile and select **Object** from the **Level** drop-down list.
4. Click **Next** to configure the data scope
5. In the **Recovery point** field, select the time from which you want to restore the objects and click **Apply**.
6. From the **Object** drop-down list, select the objects you want to restore and click **Apply**. You can view the number of records in each selected object.
7. Click **Next** to configure related data.
8. In the **Configure related data** step, configure the following settings:
    - **Restore parent and child object records** – Turn on/off the toggle to define if you want to restore parent and child object records. If you turn on the toggle, the objects you selected will be displayed as **Base** objects below. You can click any object to add its parent or child objects. Subsequently, you can also click the parent or child objects to add grandparent or grandchild objects. For the restore, you can add up to 10 levels of parent objects and 10 levels of child objects.
    - **Restore related fields for deleted records** – If the selected records do not exist in the destination organization, turn on/off the toggle to define if you want to restore these records along with the related fields of their existing first-level child object records. Note that this option is unavailable if the **Restore parent and child object records** option is enabled, and selecting it may affect the restore performance.
9. Click **Next** to configure the restore settings.
10. In the **Configure restore settings** step, configure the following settings:
    - **Where do you want to restore the data?** – Select the **Restore the data to another organization** option. Then, select a destination organization from the drop-down list.

Select a user mapping profile from the **Which user mapping profile do you want to apply** drop-down list. You can click **View details** next to the drop-down list to view the details of the user mapping profile.

You can also click **Create new** in the drop-down list to go to the user mapping page and create a new user mapping profile. For details about user mapping, refer to User Mapping.

- **Select the accuracy for restoring records** – Select to run the restore job in the **Standard precision** or **High precision**.
    - **Standard precision** can accelerate your restore progress. Using this mode, if you are about to run multiple restore jobs of the same content, there may be duplicate records. If your restore is for single-use or an urgent request, we recommend that you select this mode.

      If you plan on running the restore more than once, we recommend that you select the **High precision**.
- **How would you like to handle conflicts of restoring existing records?** – Select **Do not overwrite** if you would like to keep the current record when a conflict occurs; select **Overwrite** if you would like to keep the backup record.
- **Deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore** – Turn on/off the toggle and select the specific automation types to define if you want to deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore. They will be activated when the restore job is completed.
  You can customize the deactivation scope in job details of a pre-restore job. For detailed instructions, refer to View Job Details.
- **Restore audit fields** – Turn on/off the toggle to define if you want to restore audit fields, including **CreateById** and **CreatedDate** fields. If you select to restore, IBM® Storage Protect for Cloud Salesforce will restore the fields based on the backup values. If not, the created by user will be the user that has connected the Salesforce organization in IBM® Storage Protect for Cloud; the created time will be the restore time. Only the following object types are supported for audit field restore: **Account**, **Article Version**, **Attachment**, **Campaign Member**, **Case**, **Case Comment**, **Contact**, **Content Version**, **Contract**, **Event**, **Idea**, **Idea Comment**, **Lead**, **Opportunity**, **Question**, **Task**, **Vote**, and custom objects.

  > **Note:** To restore the audit fields, enable the **Set Audit Fields upon Record Creation** and **Update Records with Inactive Owners** permissions in Salesforce.

- **Anonymize data in the restore based on the anonymization profile** – Turn on/off the toggle to define if you would like to anonymize the backup data to high fidelity fake data generated by IBM® Storage Protect for Cloud Salesforce and restore it to your organization. When there is no enabled anonymization profile for your organization, you can click the **Settings > Profile management** link to configure one if you are the Administrator, and then click the **Refresh** button to load the profile.

  > **Note:** We do not recommend that you anonymize the data and restore it to your production organization since it may bring risks of data corruption.

11. Click **Next** to go to the **Overview** page to view the settings of the restore job.
12. Click **Restore**, and the **Restore** window appears. You can take the following actions:
    - **Pre-restore** – A pre-restore job will run according to the configurations before the actual restore. When the job is finished, you can review job recommendations in the Job Monitor. This enables you to adjust settings as needed, ensuring a smoother and error-free process.
    - **Restore** – The restore job will run directly to restore data to the destination organization. After the job has started, you can go to the Job Monitor to view more job details.

Restore Records

You can restore specific records by designating the records through recovery point, object, and keywords. The record restore is only available to the user groups that have **Restore records** permission.

> **Note:** When restoring data for custom fields that have been deleted, IBM® Storage Protect for Cloud Salesforce will re-create the custom field before restoring the data.

You can choose one of the following ways to restore the specific records:

- In Place Restore – Restore specific records to the original organization.
- Out of Place Restore – Restore specific records to another organization.

In Place Restore

Procedure

To restore specific records to the original organization, complete the following steps.

1. Click **Restore** in the left navigation.
2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.
3. Select the **Restore data** tile and select **Record** from the **Level** drop-down list.
4. Select **Backup** as the **Data Source**.
5. Click **Next** to configure the data scope.
   - If you want to search specific records, complete the following steps under the **Search mode** tab:
     a. In the **Recovery point** field, select the time from which you want to restore the records and click **Apply**.

     b. From the **Object** drop-down list, select the objects you want to restore.

     c. In the **Keyword** field, you can select to search for records by **Record name** or **Record ID**. Enter a keyword to search the records whose record name/ID contains the keyword, and click **Search**. When you search by the record name, if you want to search all records, you can enter an asterisk (*) in the text box. The default search condition is to search the backup data within the last backup cycle.
     You can click the link in the **Record ID** column to view the record details.

     d. Select the records you want to restore from the search results. If you click the checkbox next to the column name to select all the records to restore/export, all the records that meet your search conditions will be selected now, even though the records are not displayed in the search results..
     If you have the **Export** permission, you can also click **Export** to export the selected backup records to CSV files or MySQL files. If you select the records of following object types: **Attachment**, **Document**, **Static Resource**, **Mail Merge Template**, **Event Log File** and **Content Version**, you can select to export **Records** only or export **Records and files** of the objects. Note that the export job may take a long time depending on the number of records or selected time range, and it may slow down other running jobs. MySQL file format only supports exporting records, and any files will keep their original formats. The export job may take a long time depending on the number of records or selected time range, and it may slow down other running jobs. There is a monthly limit (100 GB) on the capacity of files that can be exported.
   - If you want to import multiple records from CSV files, complete the following steps under the **Import mode** tab:
     a. In the **Recovery point** field, select the time from which you want to restore the records and click **Apply**.

     b. You can click **Download CSV template** to download the CSV template file for configuring record information. Click **Browse** to import a CSV file with record information configured or a ZIP file that contains multiple CSV files.

> **Note:** In the CSV files. Only the **ID** column is required, and it must be the first column in the CSV file. Configure one record ID in each row of the column. We do not recommend that you add other columns to the file since it may slow down the restore job.

6. Click **Next** to configure related data.
7. In the **Configure related data** step, configure the following settings:
   - **Restore parent and child object records** – Turn on/off the toggle to define if you want to restore parent and child object records. If you turn on the toggle, the objects you selected will be displayed as **Base** objects below. You can click any object to add their parent or child objects. Subsequently, you can also click the parent or child objects to add grandparent or grandchild objects. For the restore, you can add up to 10 levels of parent objects and 10 levels of child objects.
   - **Restore related fields for deleted records** – If the selected records do not exist in the destination organization, turn on/off the toggle to define if you want to restore these records along with the related fields of their existing first-level child object records. Note that this option is unavailable if the **Restore parent and child object records** option is enabled, and selecting it may affect the restore performance.
8. Click **Next** to configure the restore settings.
9. In the **Configure restore settings** step, configure the following settings:
   - **Where do you want to restore the data?** – Select the **Restore the data to the original organization** option.

     In the **Select a default user for restoring records that belong to deactivated users** text box, enter a keyword of usernames to load valid users and select a default user.

     > **Note:** The default user must have the **Modify All Data** permission for the specific objects.

   - **How would you like to handle conflicts of restoring existing records?** – Select **Do not overwrite** if you would like to keep the current record when a conflict occurs; select **Overwrite** if you would like to keep the backup record.
   - **Deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore** – Turn on/off the toggle and select the specific automation types to define if you want to deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore. They will be activated when the restore job is completed.
     You can customize the deactivation scope in job details of a pre-restore job. For detailed instructions, refer to View Job Details.
   - **Restore records in the recycle bin** – Turn on/off the toggle to define if you want to restore the record from the recycle bin if the record with the same ID still exists in the recycle bin. The record ID will be kept after being restored. If you enable this feature, the record ID will be kept after being restored.
   - **Restore audit fields** – Turn on/off the toggle to defineif you want to restore audit fields, including **CreateById** and **CreatedDate** fields. If you select to restore, IBM® Storage Protect for Cloud Salesforce will restore the fields based on the backup values. If not, the created by user will be the user that has connected the Salesforce organization in IBM® Storage Protect for Cloud; the created time will be the restore time. Only the following object types are supported for audit field restore: **Account**, **ArticleVersion**, **Attachment**, **CampaignMember**, **Case**, **CaseComment**, **Contact**, **ContentVersion**, **Contract**, **Event**, **Idea**, **IdeaComment**, **Lead**, **Opportunity**, **Question**, **Task**, **Vote**, and custom objects.

     > **Note:** To restore the audit fields, enable the **Set Audit Fields upon Record Creation** and **Update Records with Inactive Owners** permissions in Salesforce.

10. Click **Next** to go to the **Overview** page to view the settings of the restore job.

11. Click **Restore**, and the **Restore** window appears. You can take the following actions:
    - **Pre-restore** – A pre-restore job will run according to the configurations before the actual restore. When the job is finished, you can review job recommendations in the Job Monitor. This enables you to adjust settings as needed, ensuring a smoother and error-free process.
    - **Restore** – The restore job will run directly to restore data to the destination organization. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

Out of Place Restore

Before you begin

If you have customized metadata configured in your source Salesforce, the customized metadata cannot be restored to another organization directly. Prior to the restore, make sure the same metadata settings are configured in the destination organization.

Procedure

To restore specific records to another organization, complete the following steps.

1. Click **Restore** in the left navigation.
2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.
3. Select the **Restore data** tile and select **Record** from the **Level** drop-down list.
4. Select **Backup** as the **Data Source**.
5. Click **Next** to configure the data scope.
    - If you want to search specific records, complete the following steps under the **Search mode** tab:
        a. In the **Recovery point** field, select the time from which you want to restore the records and click **Apply**.

        b. From the **Object** drop-down list, select the objects you want to restore.

        c. In the **Keyword** field, you can select to search for records by **Record name** or **Record ID**. Enter a keyword to search the records whose record name/ID contains the keyword, and click **Search**. When you search by the record name, if you want to search all records, you can enter an asterisk (*) in the text box. The default search condition is to search the backup data within the last backup cycle.
        You can click the **Record ID** link to view the record details.

        d. Select the records you want to restore from the search results. If you click the checkbox next to the column name to select all the records to restore/export, all the records that meet your search conditions will be selected now, even though the records are not displayed in the search results.

      If you have the **Export** permission, you can also click **Export** to export the selected backup records to CSV files or MySQL files. If you select the records of following object types: **Attachment**, **Document**, **Static Resource**, **Mail Merge Template**, **Event Log File** and **Content Version**, you can select to export **Records** only or export **Records and files** of the objects. Note that the MySQL file format only supports exporting records, and any files will keep their original formats. The export job may take a long time depending on the number of records or selected time range, and it may slow down other running jobs. There is a monthly limit (100 GB) on the capacity of files that can be exported.

    - If you want to import multiple records from CSV files, complete the following steps under the **Import mode** tab:
        a. In the **Recovery point** field, select the time from which you want to restore the records and click **Apply**.

        b. You can click **Download CSV template** to download the CSV template file for configuring record information. Click **Browse** to import a CSV file with record information configured or a ZIP file that contains multiple CSV files.

> **Note:** In the CSV files. Only the **ID** column is required, and it must be the first column in the CSV file. Configure one record ID in each row of the column. We do not recommend that you add other columns to the file since it may slow down the restore job.

6. Click **Next** to configure related data.
7. In the **Configure related data** step, configure the following settings:
   - **Restore parent and child object records** – Turn on/off the toggle to define if you want to restore parent and child object records. If you turn on the toggle, the objects you selected will be displayed as **Base** objects below. You can click any object to add their parent or child objects. Subsequently, you can also click the parent or child objects to add grandparent or grandchild objects. For the restore, you can add up to 10 levels of parent objects and 10 levels of child objects.
   - **Restore related fields for deleted records** – If the selected records do not exist in the destination organization, turn on/off the toggle to define if you want to restore these records along with the related fields of their existing first-level child object records. Note that this option is unavailable if the **Restore parent and child object records** option is enabled, and selecting it may affect the restore performance.
8. Click **Next** to configure the restore settings.
9. In the **Configure restore settings** step, configure the following settings:
   - **Where do you want to restore the data?** – Select the **Restore the data to another organization** option. Then, select a destination organization from the drop-down list.

     Select a user mapping profile from the **Which user mapping profile do you want to apply** drop-down list. You can click **View details** next to the drop-down list to view the details of the user mapping profile.

     You can also click **Create new** in the drop-down list to go to the user mapping page and create a new user mapping profile. For details about user mapping, refer to User Mapping.
   - **Select the accuracy for restoring records** – Select to run the restore job in the **Standard precision** or **High precision**.
     - **Standard precision** can accelerate your restore progress. Using this mode, if you are about to run multiple restore jobs of the same content, there may be duplicate records. If your restore is for single-use or an urgent request, we recommend that you select this mode.

       o If you plan on running the restore more than once, we recommend that you select **High precision**.
   - **How would you like to handle conflicts of restoring existing records?** – Select **Do not overwrite** if you would like to keep the current record when a conflict occurs; select **Overwrite** if you would like to keep the backup record.
   - **Deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore** – Turn on/off the toggle and select the specific automation types to define if you want to deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore. They will be activated when the restore job is completed.
     You can customize the deactivation scope in job details of a pre-restore job. For detailed instructions, refer to View Job Details.
   - **Restore audit fields** – Turn on/off the toggle to define if you want to restore audit fields, including **CreateById** and **CreatedDate** fields. If you select to restore, IBM® Storage Protect for Cloud Salesforce will restore the fields based on the backup values. If not, the created by user will be the user that has connected the Salesforce organization in IBM® Storage Protect for Cloud; the created time will be the restore time. Only the following object types are supported for audit field restore: **Account**, **ArticleVersion**, **Attachment**, **CampaignMember**, **Case**, **CaseComment**, **Contact**, **ContentVersion**, **Contract**, **Event**, **Idea**, **IdeaComment**, **Lead**, **Opportunity**, **Question**, **Task**, **Vote**, and custom objects.

> **Note:** To restore the audit fields, enable the **Set Audit Fields upon Record Creation** and **Update Records with Inactive Owners** permissions in Salesforce.

10. Click **Next** to go to the **Overview** page to view the settings of the restore job.
11. Click **Restore**, and the **Restore** window appears. You can take the following actions:
    - **Pre-restore** – A pre-restore job will run according to the configurations before the actual restore. When the job is finished, you can review job recommendations in the Job Monitor. This enables you to adjust settings as needed, ensuring a smoother and error-free process.

      •**Restore** – The restore job will run directly to restore data to the destination organization. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

Restore Fields

About this task

You can restore the values of specific fields by designating the fields through recovery point, object, and keywords. The field restore is only available to the user groups that have the **Restore fields** permission.

Procedure

To restore the values of specific fields, complete the following steps.

1. Click **Restore** in the left navigation.
2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.
3. Select the **Restore data** tile and select **Field** from the **Level** drop-down list.
4. Click **Next** to define the records for which you want to restore the fields.
    - If you want to search specific records, complete the following steps under the **Search mode** tab:
        a. From the **Object** drop-down list, select the object of the records.

        b. In the **Keyword** field, you can select to search for records by **Record name** or **Record ID**. Enter a keyword to search the records whose record name contains the keyword or enter the record ID with 18 characters, and then click **Search**. Note that the record ID is case-sensitive. Make sure the ID you enter here is consistent with the record ID in Salesforce.

        c. Select the records you want to restore from the search results.
    - If you want to import multiple records from CSV files, complete the following steps under the **Import mode** tab:
        a. From the **Object** drop-down list, select the object of the records.

        b. You can click **Download CSV template** to download the CSV template file for configuring record information. Click **Browse** to import a CSV file with record information configured or a ZIP file that contains multiple CSV files.

        > **Note:** In the CSV files. Only the **ID** column is required, and it must be the first column in the CSV file. Configure one record ID in each row of the column. We do not recommend that you add other columns to the file since it may slow down the restore job.
5. Click **Next** to select the fields you want to restore.
6. In the **Recovery point** field, select the time from which you want to restore the fields and click **Apply**.
7. Select the fields with changes you want to restore by selecting the corresponding checkboxes. You can also select the **Show unchanged fields** checkbox to view the fields without changes. Some fields are greyed out and cannot be selected because they are not supported for restoration due to Salesforce limitations.

8. Click **Next** to go to the **Overview** page to view the settings of the restore job.
9. Click **Restore** to restore the fields as your configurations. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

Restore Metadata

You can restore **AssignmentRules**, **ApexClass**, **ApexTrigger**, **ApprovalProcess**, **CustomLabels**, **CustomObject**, **Dashboard**, **EmailTemplate**, **FlexiPage**, **Flow**, **GlobalValueSet**, **Layout**, **PermissionSet**, **Profile**, **QuickAction**, **Report**, **ReportType**, **SharingRules** , **Workflow**, **DuplicateRules**, **PermissionGroups**, **Queues**, and **Tabs** metadata by designating the metadata through backup date, backup time, metadata type, and metadata name. The metadata restore is only available to user groups that have the **Restore metadata** permission.

> **Note:** In the restore job, the conflicting metadata will be overwritten by the backup metadata.

You can choose one of the following ways to restore all records in an organization:

- In Place Restore – Restore specific metadata to the original organization.
- Out of Place Restore – Restore specific metadata to another organization.

In Place Restore

Procedure

To restore the metadata to the original organization, complete the following steps.

1. Click **Restore** in the left navigation.
2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.
3. Select the **Restore metadata** tile, and then click **Next** to configure the data scope.
4. In the **Recovery point** field, select the time from which you want to restore the metadata and click **Apply**.
5. Click **Search**. All metadata in the backup will be displayed.
6. In the **Metadata type** pane, select the metadata types you want to restore. You can also search for desired metadata by entering the keyword of the metadata type in the search box.
7. In the **Metadata** pane, select the metadata you want to restore in different metadata types. You can also search for specific metadata by metadata display name or API name in the search box.

   > **Note:** Due to SOAP API limitations, metadata display names are supported only for the following metadata types: **ApexClass**, **ApexTrigger**, **EmailTemplate**, **Profile**, **Report**, **ApprovalProcess**, **PermissionSet**, and **Dashboard**.

   To ensure data completeness and accuracy, you can click **View parent metadata of the selected metadata** to view the parent metadata related to your selection. Please review the listed parent metadata and verify them in Salesforce. To successfully restore the selected metadata, ensure that the corresponding parent metadata exists in your destination organization.
8. Click **Next** to configure the restore settings.
9. In the **Configure restore settings** step, configure the following settings:
   - **Where do you want to restore the data?** – Select the **Restore the data to the original organization** option.
     In the **Select a default user for restoring records that belong to deactivated users** text box, enter a keyword of usernames to load valid users and select a default user.

     The default user must have the **Modify All Data** permission for the objects where the specific metadata resides.

- **If any metadata fails to be restored, do you want to continue to restore other successful metadata?** – Select **Roll backall metadata changes to keep the records consistent** if you would like to revert the successfully restored metadata of the object; select **Keep any successful metadata for a partial restore** if you would like to keep the successfully restored metadata of the object.
- **Revert metadata to the backup version** – Turn on/off the toggle to define if you want to revert metadata to the backup version. By enabling the toggle, IBM® Storage Protect for Cloud Salesforce will restore the metadata to your destination organization and remove any newly added fields (which were not included in the backup metadata file) from the destination.

10. Click **Next** to go to the **Overview** page to view the settings of the restore job.
11. Click **Restore** to restore the metadata as your configurations. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

Out of Place Restore

Procedure

To restore the metadata to the another organization, complete the following steps.

1. Click **Restore** in the left navigation.
2. On the **Restore** page, click the **Restore** button next to an organization that you want to restore.
3. Select the **Restore metadata** tile, and then click **Next** to configure the data scope.
4. In the **Recovery point** field, select the time from which you want to restore the metadata and click **Apply**.
5. Click **Search**. All metadata in the backup will be displayed.
6. In the **Metadata type** pane, select the metadata types you want to restore. You can also search for desired metadata by entering the keyword of the metadata type in the search box.
7. In the **Metadata** pane, select the metadata you want to restore in different metadata types. You can also search for specific metadata by metadata display name or API name in the search box.

> **Note:** Due to SOAP API limitations, metadata display names are supported only for the following metadata types: **ApexClass**, **ApexTrigger**, **EmailTemplate**, **Profile**, **Report**, **ApprovalProcess**, **PermissionSet**, and **Dashboard**.

8. To ensure data completeness and accuracy, you can click **View parent metadata of the selected metadata** to view the parent metadata related to your selection. Please review the listed parent metadata and verify them in Salesforce. To successfully restore the selected metadata, ensure that the corresponding parent metadata exists in your destination organization.
9. Click **Next** to configure the restore settings.
10. In the **Configure restore settings** step, configure the following settings:
    - **Where do you want to restore the data?** – Select the **Restore the data to another organization** option. Then, select a destination organization from the drop-down list.

      Select a user mapping profile from the **Which user mapping profile do you want to apply** drop-down list. You can click **View details** next to the drop-down list to view the details of the user mapping profile.

      You can also click **Create new** in the drop-down list to go to the user mapping page and create a new user mapping profile. For details about user mapping, refer to User Mapping.
11. Click **Next** to go to the **Overview** page to view the settings of the restore job.
12. Click **Restore** to restore the metadata as your configurations. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

User Mapping

About this task

To restore the records or objects in the out of place restore jobs, the involved source users must be mapped to the destination users. Administrators can configure the user mapping profiles. Users in other groups can only view the configured user mapping profiles.

Procedure

Complete the following steps to create a user mapping profile:

1. Navigate to **Settings** > **User mapping**.
2. Click **Create mapping profile**. The **Create a new user mapping profile** panel appears.
   - **Name** – Enter a profile name.
   - **Description** – Enter an optional description for future reference.
   - **Source organization** – Select the source organization for the user mapping profile.
   - **Destination organization** – Select the destination organization for the user mapping profile.
   - **Default destination user** – Enter a keyword of usernames to load valid users and select a default user to which to map all users that are not configured in the user mapping profile.

     > **Note:** The default user must have the **Modify All Data** permission for the specific objects or objects where the specific records reside.

   - **Mode** – To define mappings, you can either **Manually add mappings** one by one or **Import mappings from a CSV file** to add multiple mappings in bulk.
     - To manually add mappings, in the **Mapping rules** section, click **Add** to match the source users and destination users by entering the usernames in the **Source user** and **Destination user** text boxes.
     - To import mappings, in the **Mapping rules** section, click **Import**. In the Import panel, you can click **Download CSV template** to download the CSV template file for configuring user mapping information. Then, click **Browse** to select the configured CSV file. Click **Import** in the panel to add the user mappings to the **Mapping rules** section. You can also click **Export** to export the configured user mappings to update them.

       To delete mappings, you can click the delete (🗑) button next to each mapping. You can also select multiple mappings and click **Delete**.

       > **Note:** A source user can only be mapped to one destination user, but multiple source users can be mapped to the same destination user.

       > **Note:** The destination user you are about to add must have at least the same permissions as the matched source user.

3. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving any configurations. On the **User mapping** page, all configured user mapping profiles are displayed. Administrators can take the following actions on user mapping profiles:
   - Filter – Click **Filters** to filter the user mapping profiles by source and/or destination organizations.
   - Edit – Hover your mouse over a profile, click the More commands (•••) button, and select **Edit** to edit the information configured in the profile. You can also select a profile and click **Edit** to edit the profile.
   - Delete – Hover your mouse over a profile, click the More commands (•••) button, and select **Delete** to delete the profile. You can also select the profiles and click **Delete** to delete the profiles.

Create User Mapping Profiles

Procedure

Complete the following steps to create a user mapping profile:

1. Go to the **Settings** tab, and click **Manage** in the **User Mapping** area to go to the **User Mapping** page.
2. Click **Create Mapping Profile** to go to the **Create Mapping Profile** page.
3. Complete the following steps to create a user mapping profile:
   a. Select the source organization from the organization drop-down menu.

   b. In the **Profile Name** field, enter a name for the user mapping profile.

   c. In the **Description** field, enter a description for future reference.

   d. In the **Select a Destination Organization** field, select the destination organization for the user mapping profile.

   e. In the **Default Destination User** drop-down menu, select a default user to which to map all users that are not configured in the user mapping profile.

   > **Note:** The default user must have the **Modify All Data** permission to the specific objects or objects where the specific records reside.

   f. In the **Mapping List** field, click **Auto Match** to automatically match users that have the same email address. You can click the text boxes to modify the source user or destination user, or click **Remove** to remove the matched users.

   g. Click **Add** to match the source users and destination users by entering the usernames in the **Source User** and **Destination User** text boxes.

   > **Note:** A source user can only be mapped to one destination user, but multiple source users can be mapped to the same destination user

   > **Note:** The destination user you are about to add must have at least the same permissions as the matched source user.

4. Click **Save** to save this user mapping profile, or click **Cancel** to leave this page without saving any configurations

Manage User Mapping Profiles

Example

In the **User Mapping** page, all configured user mapping profiles are displayed. Administrators can perform the following actions on a user mapping profile:

> **Note:** Users in other groups can only **View** the created user mapping profiles.

- **View** – Click this button in the **Action** column of a user mapping profile to go to the **View** page. The detailed information of this user mapping profile is displayed.
- **Edit** – Click this button in the **Action** column of a user mapping profile to go to the **Edit** page and edit the profile name, description, selected organization, default user, and mapping list of this user mapping profile. For more detailed information about creating user mapping profiles, refer to Create User Mapping Profiles.

- **Delete** – Click this button in the **Action** column of a user mapping profile to delete it.

Perform Sandbox Seeding

About this task

IBM® Storage Protect for Cloud Salesforce allows you to create templates to define the objects you want to seed and run sandbox seeding jobs to seed the data of the objects to your sandbox organization. The **Sandbox Seeding** feature is only available to the users in the groups that have the **Sandbox seeding** permission.

Before the actual sandbox seeding, you can run a pre-seeding and review job recommendations in the Job Monitor. This enables you to adjust settings as needed, ensuring a smoother and error-free process.

Procedure

To perform sandbox seeding, complete the following steps:

1. Click **Sandbox seeding** in the left navigation.
2. Click **Create template** to create a template.
   When you first access the sandbox seeding function, click **Start now** to create a template.
3. Complete the general information for the template you are about to create:
   - **Name** – Enter a name for the template.
   - **Description** – Enter an optional description for future reference.
   - **Source organization** – Select an organization from the drop-down list to define where you want to seed the data from.
   - **Destination organization** – Select an organization from the drop-down list to define where you want to seed the data.
   - **Configure user mapping** – Turn on/off the toggle to define if you want to configure using mapping for the template. If you turn on the toggle, take the following actions according to different conditions:
     - If the destination organization you selected is a **production organization**, select a user mapping profile from the drop-down list. You can click **View** to view the details of the user mapping profile. You can also click the **Create new** option in the drop-down list to go to the user mapping page and create a new user mapping profile. For details about user mapping, refer to User Mapping.
     - If the destination organization you selected is a **sandbox organization**, you can take the following actions:
       - **Use the original user information in the destination organization** – Once enabled, users in the destination organization will be generated based on the source organization's user data during the initial template setup. User licenses will be allocated to the generated users.
         In the **Indicate the desired suffix for the username to be generated in the destination organization** text box, you can enter a suffix for the username to be generated in the destination organization to prevent any issues with duplicate usernames. For instance, if the original username is user1@example.com and the suffix "test" is added, it will appear as user1@example.com.test in the destination organization.
       - **Select a user mapping profile** – Select a user mapping profile from the drop-down list. You can click **View** to view the details of the user mapping profile. You can also click the **Create new** option in the drop-down list to go to the user mapping page and create a new user mapping profile. For details about user mapping, refer to User Mapping.
4. Click **Next** to select the data scope.
5. Click **Add object**. In the **Add object** panel, select an object you want to include in the template.
   - To seed all backup records of the selected object, select **All backup records**
   - To filter records by the backup date, select **Filter by backup date range** and enter a positive integer to only include records backed up within specific days.

- To seed the records recently generated in the backup data, select the **Select the count of backup records** option, and then enter a number.
- To import multiple records from a CSV/ZIP file, select the **Import record IDs/names of the backup records by a CSV/ZIP file**. You can click **Download CSV template** to download the CSV template file for configuring record information. Click **Upload** to import a CSV file with record information configured or a ZIP file that contains multiple CSV files.
- Click **Add** to add the object.

  In the object list, you can hover your mouse over an object, click the More (•••) commands button, and select **Edit** or **Delete** to edit or delete the added object.

  When editing an object, you can click **Add condition** and follow the steps to add field-level conditions to filter the records for seeding:

  a. Select a field of the object and then select an operator.

  b. Enter a value for the filter.

  c. Click the Add (+) icon next to the condition and repeat the steps above to add more conditions.
  You can configure conditions using **And** or **Or**. With **And**, all conditions must be met; with **Or**, any one of the conditions can be met.

  d. You can click **Add condition group** to add a new condition group. You can configure conditions using **And** or **Or**. With **And**, all condition groups must be met; with **Or**, any one of the condition groups can be met.

  e. Click **Save** to apply the conditions. Objects filtered by field-level conditions will be marked as **field-level filtered** in the **Data scope** column.

6. Click **Next** to configure related data.
7. In the **Configure related data** step, turn on/off the **Seed parent and child object records** toggle to define if you want to restore parent and child object records. If you turn on the toggle, the objects you selected will be displayed as **Base** objects below. You can click any object to add its parent or child objects. Subsequently, you can also click the parent or child objects to add grandparent or grandchild objects. For the restore, you can add up to 10 levels of parent objects and 10 levels of child objects.
8. Click **Next** to configure the settings for sandbox seeding.
   - **Seeding methods** – Select one of the following seeding methods:
     - **Insert** – Seed only records that do not already exist in the destination. Existing records in the destination will remain unchanged.
     - **Upsert** – Seed records that do not already exist in the destination. Existing records in the destination will be replaced with the backup data.
     - **Delete and insert** – Delete all existing data of the configured objects from the sandbox before seeding. Then seed new records as configured in the template. You can select to delete only the records of the objects configured in the template or delete the records of the configured objects together with the selected related records in the template.
   - **Deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore** – Turn on/off the toggle and select the specific automation types to define if you want to deactivate related triggers, flows and processes, workflow rules, and validation rules during the restore. They will be activated when the restore job is completed.
   - **Anonymize your data in the sandbox seeding job based on the anonymization profile** – Turn on the toggle if you would like to anonymize the backup data to high fidelity fake data generated by IBM® Storage Protect for Cloud Salesforce and seed it to your sandbox organization. When there is no enabled anonymization profile for your organization, you can click the **Settings > Profile management** link to configure one if you are the Administrator, and then click the **Refresh** button to load the profile.
9. Click **Next** to view the configurations of the template on the **Overview** page. Then you can take the following actions:
   - **Save** – Save the template.

- **Back** – Go back to the previous page.
- **Save and run now** – Seed the objects that match your configurations. The **Sandbox seeding** window appears and you can take the following actions:
    - **Pre-seeding** – A pre-seeding job will run according to the configurations before the actual restore. When the job is finished, you can review job recommendations in the Job Monitor. This enables you to adjust settings as needed, ensuring a smoother and error-free process.
    - **Seeding** – The sandbox seeding job will run directly to seed data to the destination organization. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

After you add a template, you can manage the templates of all organizations on the **Sandbox seeding** page:

- View – Click the template name link to view the details.
- **Edit** – Hover your mouse over a template, click the More commands (•••) button, and select **Edit** to edit the template.
- **Delete** – Hover your mouse over a template, click the More commands (•••) button, and select **Delete** to delete the template.
- **Configure schedule** – Hover your mouse over a template, click the More commands (•••) button, and select **Configure schedule** to configure schedule settings. To enable scheduled seeding, turn on the **Enable scheduled seeding** toggle and configure the following settings:
    - **Start time** – Select the start time of the schedule, and the first sandbox seeding on the template will be automatically performed at that start time.
    - **Interval** – Configure the interval for the scheduled sandbox seeding.
- **Run** – Click **Run** next to a template to run a pre-seeding or actual sandbox seeding job for the organization based on the template. The **Sandbox seeding** window appears and you can take the following actions:
    - **Pre-seeding** – A pre-seeding job will run according to the configurations before the actual restore. When the job is finished, you can review job recommendations in the Job Monitor. This enables you to adjust settings as needed, ensuring a smoother and error-free process.
    - **Seeding** – The sandbox seeding job will run directly to seed data to the destination organization. After the job has started, you can go to the job monitor to view more job details. For details, refer to Job Monitor.

Configure Settings

Refer to the following instructions to configure settings for IBM® Storage Protect for Cloud Salesforce:

- Manage Accounts to determine who is going to administer the backup and provide access to them. Administrators can add users into different groups and edit the user permissions by managing groups in Salesforce Backup.
- Configure a Custom Storage Location and Database to store the backup data if you have the **Bring your own storage** option on your Salesforce Backup subscription.
- Configure Data Retention Settings to define the retention period of your backup data in the storage.
- Configure the Encryption Profile to protect your backup data using the security keys generated by the encryption method.
- Configure Data Anonymization Profiles if you want to anonymize the backup data in the Restore Objects or Restore Organization jobs.
- Configure Notifications to define the settings of email notifications sent by Salesforce Backup.
- Manage Organizations to view and edit the basic information of your organizations.
- Configure API Usage Limit to pause the jobs when your Salesforce API usage exceeds the limit you configure.
- Configure Bulk API Usage to define the usage of Bulk API and Bulk API 2.0 and configure the usage limits.

Manage Users

The account that created an app profile will become the tenant owner of it and a Service Administrator in IBM® Storage Protect for Cloud automatically; this account will be added into the Administrators group in IBM® Storage Protect for Cloud Salesforce automatically.

About this task

Only administrators can add users into different groups and edit the user permissions by managing groups.

Administrators can create custom groups and edit group permissions for managing the users who will use IBM® Storage Protect for Cloud Salesforce.

Procedure

Complete the following steps to create a group and grant permissions to it:

1. Navigate to **Settings › User management**.
2. On the **User management** page, click **Create security group**. The **Create a new security group** panel appears.
3. Configure the following settings:
   - **Name** – Enter a group name.
   - **Description** – Enter an optional description for future reference.
   - **Invite users** – Enter the users or groups that you want to add to this group in the text box.
   - **Select organization scope** – Select the organizations whose data can be managed by the users in the group. You can click **Select all** to allow this group to manage all organizations.
   - **Select permission scope** – Select permissions of features for the group. Each feature is only available to the groups that have the corresponding permission. For more detailed information about permissions, refer to "Appendix A - Permissions" on page 85.
     After selecting the **Discover** permission, administrators can also define the object scope for users to run the Discover job. You grant access to all objects in the selected organization or a custom object scope.

4. Click **Save** to save your configurations, or click **Cancel** to leave the page without saving any configurations.
   On the **User management** page, administrators can take the following actions on a group:
   - View – Click the group name link to view the details in the panel.
   - Edit – Select a group and click **Edit** to edit the name, description, user, and permissions of this group.
   - Delete – Select the groups and click **Delete** to delete the groups.

Configure a Custom Storage Location and Database

When **Bring your own storage** is selected in the subscription of IBM® Storage Protect for Cloud Salesforce, administrators can configure a custom storage location to store the files and configure a database to store the records and relational data of the backup data.

Procedure

If you have purchased a subscription for BYOS (Bring your own storage) but are currently using IBM default storage for your backup data, your backup jobs will fail, and we will send you an email notification every 7 days to remind you to update your BYOS storage configuration.

Complete the following steps to configure the custom storage location and database:

1. Navigate to **Settings › Storage**.
2. Click **Storage**. All organizations that you manage are displayed in the panel. You can click the down arrow (⌄) button next to an organization to view the storage location details.
   After the administrator’s login, the **Startup wizard**page will appear if the storage location and database have not been configured. You can turn on the toggle of an organization to configure the storage information.

   For distributor customers, after the administrator’s login, , the **Startup wizard**page will appear if they have not been configured. You can turn on the toggle of an organization to use **IBM® Storage Protect for Cloud default storage** or select **Bring your own storage** to configure a custom storage location and database.
3. Click the edit (✏) button next to the organization you want to manage.
4. Select the storage type you want to use and configure the settings. The **Microsoft Azure Storage**, **SFTP**, **Amazon S3**, **Amazon S3-Compatible Storage**, **IBM® Storage Protect - S3**, and **IBM Cloud Object Storage** types are supported.
   With **Microsoft Azure Storage** selected, configure the following settings to configure the storage location and database:
   - **Access Point** – Enter the URL for the Storage Service.
   - **Account Name** – Enter the corresponding account name to access the specified storage.
   - **Account Key** – Enter the corresponding account key to access the specified storage.
   - **Extended parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
     - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
       If you do not configure this parameter, the value is 30000 milliseconds by default.
     - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 times.

       If you do not configure this parameter, the value is 6 by default.

  - **CustomizedMetadata={}** – User-added metadata is supported. Configure the metadata in the parameter. For example: **CustomizedMetadata={[testKey1,testValue1],[testKey2,testValue2],[testKey3,testValue3]}**.
  - **CustomizedMode=Close** – User-added metadata is not supported.

With **SFTP** selected, configure the following settings to configure the storage location:

- **Host** – Enter the IP address of the SFTP server.
- **Port** – Enter the port to use to connect to this SFTP server.
- **Root Folder** – Enter the root folder where you wish to access.
- **Username**– Enter the username used to access the root folder.
- **Password** – Enter the corresponding password of the user used to access the root folder.
- **Private Key** – If the SFTP server supports the private key, enter the private key here.
- **Private Key Password** – Enter the corresponding password of the private key.

With **Amazon S3** selected, configure the following settings to configure the storage location:

- **Bucket Name** – Enter the bucket name you wish to access.
  Note the following:
  - If the entered name doesn't match an existing bucket, a new bucket will be automatically created.
  - Ensure the bucket policy in Amazon S3 storage applied to your account contains the following required permissions:
    - **Read**: Get Object
    - **List**: ListBucket
    - **Write**: DeleteObject; PutObject; DeleteObjectVersion
- **Access Key ID** – Enter the corresponding access key ID to access the specified bucket. You can view the **Access key ID** from your AWS account.

  > **Note:** The AWS account must have the AmazonS3FullAccess policy assigned.

- **Secret Access Key** – Enter the corresponding secret key ID to access the specified bucket. You can view the **Secret Access Key** from your AWS account.
- **Storage Region** – Select the **Storage Region** of this bucket from the drop-down menu. The available regions are

US East (N. Virginia)	US East (Ohio)	US West (Northern California)
US West (Oregon)	Canada (Central)	EU (Ireland)
EU (Frankfurt)	EU (London)	Asia Pacific (Singapore)
Asia Pacific (Tokyo)	Asia Pacific (Sydney)	Asia Pacific (Seoul)
Asia Pacific (Mumbai)	South America (Sao Paulo).	

- **Extended parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameter
  - **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds. If you do not configure this parameter, the value is 30000 milliseconds by default.
  - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 times. If you do not configure this parameter, the value is 6 by default.

    - **CustomizedMetadata** – Configure if customized metadata or user-added metadata is supported. By default, customized metadata and user-added metadata are all supported.
    - **CustomizedMode=Close** – This physical device will not support customized metadata or user-added metadata.
    - **CustomizedMode=SupportAll** – This physical device will support all customized metadata and user-added metadata.
    - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.
    - **CustomizedRegion** – Configure the customized region of the physical device. For example, enter **CustomizedRegion=s3-us-gov-west-1.amazonaws.com** to configure the GovCloud account.

With **Amazon S3-Compatible Storage** selected, configure the following settings to configure the storage location:

- **Bucket name** – Enter the bucket name you wish to access.
  Note the following:
    - If the entered name doesn't match an existing bucket, a new bucket will be automatically created.
    - Ensure the bucket policy in Amazon S3 storage applied to your account contains the following required permissions:
        - **Read**: Get Object
        - **List**: ListBucket
        - **Write**: DeleteObject; PutObject; DeleteObjectVersion
- **Access Key ID** – Enter the corresponding access key ID to access the specified bucket.
- **Secret Access Key** – Enter the corresponding secret key ID to access the specified bucket.
- **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

  > **Note:** The URL must begin with **http://** or **https://**.

- **Extended parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
    - **SignatureVersion** – By default, IBM® Storage Protect for Cloud Salesforce uses V4 authentication to access your storage. If you want to use V2 authentication, add **SignatureVersion=2** into the extended parameters.
    - **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
      If you do not configure this parameter, the value is 30000 milliseconds by default.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 times.
      If you do not configure this parameter, the value is 6 by default.
    - **CustomizedMetadata** – Configure if customized metadata or user-added metadata is supported. By default, customized metadata and user-added metadata are all supported.
    - **CustomizedMode=Close** – This physical device will not support customized metadata or user-added metadata.
    - **CustomizedMode=SupportAll** – This physical device will support all customized metadata and user-added metadata.
    - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.

With **IBM Storage Protect- S3** selected, configure the following settings to configure the storage location and database:

- **Bucket name** – Enter the bucket name you wish to access.
  Note the following:
  - The IBM Storage Protect Object client (S3) must be installed and configured before setting up IBM® Storage Protect for Cloud. Refer to, Sending data from other object clients to IBM Storage Protect.
  - The entered name must match an existing bucket. For details on creating a bucket, see How to create an S3 bucket in IBM Storage Protect.
  - Ensure the bucket policy in Amazon S3 storage applied to your account contains the following required permissions:
    - **Read**: Get Object
    - **List**: ListBucket
    - **Write**: DeleteObject; PutObject; DeleteObjectVersion
- **Access key ID** – Enter the corresponding access key ID to access the specified bucket.
- **Secret Access Key** – Enter the corresponding secret key ID to access the specified bucket.
- **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

  > **Note:** The URL must begin with "http://" or "https://".

- **Extended parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
  - **Allow_Insecure_SSL** – By default, the storage client expects an SSL certificate issued by a public trusted certificate authority over HTTPS transport to ensure integrity. A self-signed certificate on the storage server side will fail the certificate validation. If you choose to use a self-signed certificate, you can set the **Allow_Insecure_SSL** to **true** in the **Extended parameters** to bypass the certificate validation
  - **SignatureVersion** – By default, IBM® Storage Protect for Cloud Salesforce uses V4 authentication to access your storage. If you want to use V2 authentication, add **SignatureVersion=2** into the extended parameters.
  - **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
    If you do not configure this parameter, the value is 30000 milliseconds by default.
  - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 times.
    If you do not configure this parameter, the value is 6 by default.
  - **CustomizedMetadata** – Configure if customized metadata or user-added metadata is supported. By default, customized metadata and user-added metadata are all supported.
  - **CustomizedMode=Close** – This physical device will not support customized metadata or user-added metadata.
  - **CustomizedMode=SupportAll** – This physical device will support all customized metadata and user-added metadata.
  - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.
  - **Cert_thumbprint** - If you have a self-signed certificate for S3 server and only want to pass the certificate validation with a specific thumbprint, enter your thumbprint as the value of the parameter.

With **IBM Cloud Object Storage** selected, configure the following settings to configure the storage location and database:

- **Bucket name** – Enter the bucket name that you wish to access.
  Note the following:
  - If the entered name doesn't match an existing bucket, a new bucket will be automatically created.
  - Ensure the bucket policy in Amazon S3 storage applied to your account contains the following required permissions:
    - **Read**: Get Object
    - **List**: ListBucket
    - **Write**: DeleteObject; PutObject; DeleteObjectVersion
- **Access key ID** – Enter the corresponding access key ID to access the specified bucket.
- **Secret access key** – Enter the corresponding secret key ID to access the specified bucket.
- **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

  > **Note:** The URL must begin with "http://" or "https://".

- **Extended parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
  - **SignatureVersion** – By default, IBM® Storage Protect for Cloud Salesforce uses V4 authentication to access your storage. If you want to use V2 authentication, add **SignatureVersion=2** into the extended parameters.
  - **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds. If you do not configure this parameter, the value is 30000 milliseconds by default.
  - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 times. If you do not configure this parameter, the value is 6 by default.
  - **CustomizedMetadata** – Configure if customized metadata or user-added metadata is supported. By default, customized metadata and user-added metadata are all supported.
  - **CustomizedMode=Close** – This physical device will not support customized metadata or user-added metadata.
  - **CustomizedMode=SupportAll** – This physical device will support all customized metadata and user-added metadata.
  - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.

5. Configure the following settings to configure the database:

   > **Note:** The Enterprise edition of SQL Server 2014 or later is supported for the database. You can use either an online SQL server or an on-premises SQL server with the Enterprise edition. Ensure that IBM® Storage Protect for Cloud Salesforce can connect to the SQL server. We recommend that you add the reserved IP address of IBM® Storage Protect for Cloud Salesforce to the allowed list of your SQL server firewall. To download the reserved IP address, go to IBM® Storage Protect for Cloud > **Advanced Settings** > **Reserved IP Addresses** > **Download a List of Reserved IP Addresses**.
   >
   > - **Instance Name** – Enter the instance name of the SQL server where the database resides.

- **Database Name** – Enter the name of an existing database you want to use.
- **Authentication method**– Select an authentication method from **SQL authentication** and **Microsoft Entra authentication**.
- **Username** – Enter the username of the account that has the **db_owner** role of the above database.
- **Password** – Enter the password of the above account.
- **Encrypt connection** – Turn on/off the toggle to define if you want to encrypt the server certificate. The feature is enabled by default.
- **Trust server certificate** – Turn on/off the toggle to define if you want to trust the server certificate.
- **Certificate file (.cer) -** If your SQL server is protected by a custom SSL certificate, upload the certificate file to connect to your server.

  > **Note:** If you use the Amazon RDS for SQL Server and use the built-in certificate, the certificate file is not required here.

6. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving any configurations. If you are on the **Startup wizard** page, click **Back up now** to start the backup jobs for the configured organizations.

How to Allow IBM® Storage Protect for Cloud Products to Access Your Storage

If you are using or plan to use your own storage, read the instructions in this section carefully and complete the settings upon your need. Otherwise, you can skip this topic.

When you are using your own storage device, you may have set up the storage firewall to only allow the trusted clients for security concerns. To ensure that IBM® Storage Protect for Cloud products can access your storage, complete the settings as required in the following conditions:

> **Note:** If you are using a trial subscription and the storage account you want to use in the trial has a firewall enabled, read the conditions below and contact IBM Software Support for the corresponding reserved IP addresses or ARM VNet IDs.

- If you are using a storage type other than Microsoft Azure storage, you must add reserved IP addresses to your storage firewall. To get the list of the reserved IP addresses, refer to Download a List of Reserved IP Addresses.
- If you are using Microsoft Azure storage, refer to the following:
  - If your storage account is in the same data center as the one you use to sign up for IBM® Storage Protect for Cloud or your storage account is in its paired region**,** you must add the Azure Resource Manager (ARM) vNet subnets where the IBM® Storage Protect for Cloud agents are running on to your storage networking. You can find additional details in this Microsoft article: Grant access from a virtual network. To get the ARM VNet subnet IDs for your data center, go to IBM® Storage Protect for Cloud > **Advanced Settings** > **Firewalls and Virtual Networks**. For detailed instructions, refer to "Add ARM Virtual Networks" on page 52.
  - **Other than the condition above**, you need to add all reserved IP addresses to the Azure storage firewall. For details, refer to "Add Reserved IP Addresses" on page 52.

Add Reserved IP Addresses

Procedure

Follow the below steps to Add Reserved IP Addresses:

1. Navigate to **IBM® Storage Protect for Cloud** interface > **Advanced Settings**> **Reserved IP Addresses** to download the list of reserved IP addresses of IBM® Storage Protect for Cloud. For details, refer to Download a List of Reserved IP Addresses.
2. Go to the storage account that you want to secure.
3. Select **Networking** on the menu.
4. Check that you've selected to allow access from **Selected networks**.
5. Enter the IP address or address range under **Firewall › Address Range**.
6. Select **Save** to apply your changes.

Add ARM Virtual Networks

To grant access to a subnet in a virtual network belonging to another tenant, use PowerShell, CLI, or REST API.

> **Note:** To get the subnet ID of IBM® Storage Protect for Cloud products for your data center, go to IBM® Storage Protect for Cloud > Administration > Security > ARM VNet IDs.

- Get the IBM® Storage Protect for Cloud products network subnet resource ID

```
$SUBNETID="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy/resourceGroups/
ResrouceGroupName/providers/Microsoft.Network/virtualNetworks/VIrtualNetworkName/
subnets/SubnetName"

$DESTRG="customer_resource_group_name"
$DESTSTA="customer_storage_account_name"
```

- Use the Azure CLI tool (https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest)

```
# Step 1 (Optional): If you have multiple Azure subscriptions, please switch to the
correct subscription
# This command sets the active subscription to the specified subscription ID.
az account set --subscription xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy

# Step 2 (Optional): Confirm whether the subscription switch is correct
# This command displays the current subscription information in a table format.
az account show --output table

# Step 3: Get the IBM® Storage Protect for Cloud network subnet resource ID
# This variable stores the resource ID of the subnet in the virtual network.
# Replace with the Azure Resource Manager (ARM) VNet ID downloaded from
your IBM® Storage Protect for Cloud tenant.
$SUBNETID="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy/resourceGroups/
ResourceGroupName/providers/Microsoft.Network/virtualNetworks/VirtualNetworkName/
subnets/SubnetName"

# Step 4: Set your resource group name
# This variable stores the name of the resource group where your storage account is
located.
$DESTRG="customer_resource_group_name"

# Step 5: Set your storage account name
# This variable stores the name of the storage account to which you want to add the
network rule.
$DESTSTA="customer_storage_account_name"

# Step 6: Add the firewall virtual network rule to grant access to IBM® Storage Protect
for Cloud
# This command adds a network rule to the specified storage account, allowing access
from the specified subnet.
az storage account network-rule add --resource-group $DESTRG --account-name $DESTSTA --
subnet $SUBNETID
```

```
# Step 7: List the current network rules for the storage account to verify the addition
# This command lists the virtual network rules for the specified storage account.
az storage account network-rule list --resource-group $DESTRG --account-name $DESTSTA
--query virtualNetworkRules

# Step 8 (Optional): Disable the public access to storage account
# This command updates the storage account to deny public network access.
az storage account update --resource-group $DESTRG --name $DESTSTA --default-action
Deny

# Step 9 (Optional): Verify that the default action for network rules is set to Deny
# This command shows the network rule set for the specified storage account, including
the default action.
az storage account show --resource-group $DESTRG --name $DESTSTA --query
networkRuleSet.defaultAction
```

- Use the Azure Az PowerShell Module (https://learn.microsoft.com/en-us/powershell/azure/install-azure-powershell?view=azps-14.2)

```
# Step 1: Sign in to Azure with your Azure Admin account
Connect-AzAccount

# Step 2 (Optional): If you have multiple Azure subscriptions, please switch to the
correct subscription
# This command sets the active subscription to the specified subscription ID.
Set-AzContext -SubscriptionId "xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy"

# Step 3: Get the IBM® Storage Protect for Cloud network subnet resource ID

# This variable stores the resource ID of the subnet in the virtual network.

# Replace with the Azure Resource Manager (ARM) VNet ID downloaded from
your IBM® Storage Protect for Cloud tenant.
$SUBNETID="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy/resourceGroups/
ResourceGroupName/providers/Microsoft.Network/virtualNetworks/VirtualNetworkName/
subnets/SubnetName"

# Step 4: Set resource group name
# This variable stores the name of the resource group where your storage account is
located.
$DESTRG="customer_resource_group_name"

# Step 5: Set storage account name
# This variable stores the name of the storage account to which you want to add the
network rule.
$DESTSTA="customer_storage_account_name"

# Step 6: Add the firewall virtual network rule to grant access to IBM® Storage Protect
for Cloud
# This cmdlet adds a network rule to the specified storage account, allowing access
from the specified subnet.
Add-AzStorageAccountNetworkRule -ResourceGroupName $DESTRG -Name $DESTSTA
-VirtualNetworkResourceId $SUBNETID

# Step 7: Verify the newly added network rule.

# This cmdlet retrieves the network rule set for the specified storage account.

Get-AzStorageAccountNetworkRuleSet -ResourceGroupName $DESTRG -AccountName
```

You will see the virtual network rules in Azure Portal. You may also notice that a warning message "Insufficient Permission..." is displayed. It is because the subnet is not in your subscription. You can ignore it.

Configure Data Retention Settings

Either using the IBM® Storage Protect for Cloud default storage or your custom storage, the data retention period can be applied to your backup data to help save your storage costs. Once the backup data reaches the data retention date, it will be deleted from the storage. Administrators can configure the data retention period of an organization.

Procedure

> **Note:** After updating the data retention period for an organization, if the retention date has already passed, backup data will be retained for an additional 90 days. Email notifications will be sent before deletion.

Complete the following steps to configure the data retention settings:

1. Navigate to **Settings › Storage**.
2. Click **Retention**. All organizations that you manage are displayed in the panel.
3. Select a number or select **Unlimited** to define the retention period of your backup data. The unit is year.
4. Click **Apply** to save the configurations.
   You can download the retention job report in the **Job monitor** when the job is finished.

Configure the Encryption Profile

Encryption profiles can protect your backup data using the security keys. The default encryption profile for IBM® Storage Protect for Cloud Salesforce is used if you do not configure a custom one.

Procedure

> **Note:** Encryption profile configuration will not be supported in IBM® Storage Protect for Cloud Salesforce soon. We recommend that you switch to configure the encryption profile in IBM® Storage Protect for Cloud. For more information about encryption profiles, refer to the IBM Storage Protect for Cloud User Guide.

Administrators can complete the following steps to manage the encryption profile in IBM® Storage Protect for Cloud Salesforce:

1. Navigate to **Settings › Storage**.
2. Click **Encryption profile**.
   - If you have not configured the encryption profile for an organization, click the **Configure** button next to it to use the default encryption profile in IBM® Storage Protect for Cloud.
   - If you have configured the encryption profile for an organization in the legacy experience, you can click **Change** next to it to change to use the default encryption profile in IBM® Storage Protect for Cloud.
   - The new organizations managed by IBM® Storage Protect for Cloud Salesforcewill use the encryption profile that is used in IBM® Storage Protect for Cloud and cannot be changed.

> **Note:** If you change to use a different encryption profile in IBM® Storage Protect for Cloud, the old backup data of IBM® Storage Protect for Cloud Salesforce is still protected by the original encryption profile. Thus, make sure the original encryption profile is not deleted, and your key vault is available in Azure. You can delete the original encryption profile if you are sure that the old backup data is no longer needed.

Configure Data Anonymization Profiles

Procedure

Administrators can configure data anonymization profiles for different field values of different objects. Then, users can anonymize data in the organization restore, object restore, and sandbox seeding jobs based on the pre-configured templates. For the supported and unsupported fields in data anonymization, refer to "Appendix E - Supported and Unsupported Fields in Data Anonymization and Cleanup" on page 125.

Complete the following steps to configure the templates:

1. Navigate to **Settings › Profile management**.
2. Click the **Anonymization profile** tab.
3. Under a desired organization section, click **Create profile**. The **Create a new anonymization profile** panel appears.
4. Select an object from the drop-down list.
5. Select a language from the drop-down list to anonymize the sensitive information with the random values in that language.
6. Turn on/off the toggle in front of the fields to enable or disable the fields for anonymization. You can also search a field by entering the field name in the search box.
7. Select an anonymization type for each field. The field value will be anonymized using a random value of that type. If you select **Custom value**, enter a value in the text box.

   > **Note:** Select correct anonymization types for fields to ensure you are mapping high-fidelity responses for data fields and the data can be restored. For example, if you select the **Random date and time** anonymization type, make sure the field supports the date or time format.

   > **Note:** The data after anonymization for different fields of a record may not match. For example, if you anonymize two fields using Country and City, the city after anonymization for one record may not belong to the country.

8. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving the configurations. After you add anonymization profiles, you can perform the following actions to manage the profiles:
   - View – Click the **Anonymize {number} fields** link in the **Configuration status** column to view the details.
   - Edit – Select a profile and click **Edit** to edit the profile.
   - Delete– Select the profiles and click **Delete** to delete the profiles.

Configure Notifications

In IBM® Storage Protect for Cloud Salesforce, you can define certain statuses of backup, restore, and sandbox seeding jobs which will trigger alerts and define whether to trigger notifications for export, data cleanup, and data retention.

Procedure

To create a notification profile, complete the following steps:

1. Navigate to **Settings › Notification**.
2. Click **Create notification profile**. The **Create a notification profile** panel appears.
3. Configure the following settings:
   - **Name** – Enter a name for the notification profile.
   - **Description** – Enter an optional description for future reference.
   - **Send email notifications to the user who connects the Salesforce organization** – This setting is only available for the notification profiles created before with this setting enabled. You can turn off the toggle to disable the setting if you do not want to send email notifications to the user who has connected the organization in IBM® Storage Protect for Cloud . Once the setting is disabled, the option will not be shown the next time you edit this notification profile. If you want to enable the email notification to the user who connects to the Salesforce organization after that, you can enter the user in the text box.

- **Send email notifications to the following email addresses** – Enter the email addresses in the text box to configure the recipients for the email notifications. You can enter the email addresses of users or groups. For groups, you must ensure the group you entered can receive emails. Otherwise, the group members will not be notified.
- **Select organization scope** – Select the organizations that will use this notification profile. You can click **Select all** to use this profile for all organizations.
- **Send the email notifications for the jobs in the following statuses** – Select the job statuses for the backup, restore, sandbox seeding and compare jobs which will trigger the notifications. Select whether you want to trigger notifications when a potential ransomware attack is detected, or unusual activities are detected and whether to trigger notifications for completed data export, data cleanup, data discover,data service, and data retention (delete the backup job based on the retention settings) jobs.

4. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving the configurations. After you add notification profiles, you can perform the following actions to manage the profiles:
    - View – Click the link to view the details.
    - Edit – Select a profile and click **Edit** to edit the profile.
    - Delete– Select the profiles and click **Delete** to delete the profiles.

Manage Organizations

The **Organization management** page allows administrators to view the basic information of the organizations that they can manage.

Navigate to **Settings › General**, and then click **Organization management**. All organizations you manage are displayed in the panel. View the organization name, display name, and status. You can update the display name of each organization in IBM® Storage Protect for Cloud Salesforce.

If you no longer need to manage an organization in IBM® Storage Protect for Cloud Salesforce, you can delete the organization together with the backup data, templates, jobs, profiles, and data service of the organization.

Click the delete (🗑) button next to the organization, and click **Delete** in the confirmation window to delete the organization. If you do not need to delete organizations and want to disable the function, contact IBM Software Support for assistance.

If you would like to use IBM® Storage Protect for Cloud Salesforce to protect Salesforce data in other organizations, you need to connect your Salesforce organization in IBM® Storage Protect for Cloud Salesforce, and then create a IBM® Storage Protect for Cloud Salesforce app profile for the organization. After an app profile of an organization is created, the organization is registered into IBM® Storage Protect for Cloud Salesforce automatically. You can click the **IBM Storage Protect for Cloud > Tenant management** link on the page to connect your organization. For detailed information, refer to the IBM Storage Protect for Cloud User Guide.

> **Note:** If you have deleted a Salesforce organization from an IBM® Storage Protect for Cloud tenant and connected the organization to another IBM® Storage Protect for Cloud tenant, the organization may not be displayed in the new IBM® Storage Protect for Cloud Salesforce environment. Before connecting the organization to the new tenant, contact IBM Software Support for assistance.

Configure API Usage Limit

Administrators can configure a percentage for Salesforce API usage limits in Settings. When the API usage of your organization within 24 hours exceeds the percentage, the jobs in IBM® Storage Protect for Cloud Salesforce will be automatically paused. When there is enough API quota, the jobs will be resumed.

Procedure

The total number of API requests allowed by Salesforce is defined by the users' licenses in the organization. For details, refer to the Salesforce documentation: API Request Limits and Allocations. For your current API usage, navigate to Salesforce > **System Overview** > **API Usage**.

Complete the following steps to configure the API usage limit in IBM® Storage Protect for Cloud Salesforce:

1. Navigate to **Settings › General**.
2. Click **API usage limit**.
3. In the **API usage limit** panel, enter an integer from 1 to 100 in the text box of an organization to define the percentage. Make sure you set an appropriate value to ensure your jobs will not be affected.
4. Click **Apply** to save the configurations.

Configure Bulk API Usage

Any job processes that include more than 2,000 records are good candidates for Bulk API 2.0 to successfully prepare, execute, and manage an asynchronous workflow using the Bulk framework . Administrators can enable Bulk API and configure its limitations as needed. The jobs will be executed using Bulk API.

About this task

When the Bulk API reaches its limit, we will automatically switch to using the SOAP API for backup. If the API usage of your organization exceeds the percentage of the API limit within a 24-hour period, jobs will be paused in the backend and will resume once there is sufficient API quota available.

Procedure

Complete the following steps to configure the Bulk API usage:

1. Navigate to **Settings** > **General**.
2. Click **Bulk API Usage** . All organizations that you manage are displayed in the panel.
3. Turn on the toggle next to the organization you desired, and the **Configure Bulk API usage** panel appears.
4. Enter a value in the **Bulk API backup threshold** field. When the number of records in a backup job or in the backup process exceeds this limit, Bulk API and Bulk API 2.0 will be used for the job. The default value is 2,000.

   > **Note:** For restore or sandbox seeding jobs, the Bulk API will be used once it is enabled.

5. Then configure the following settings:
   - **Enable Bulk API** – Turn on/off the toggle to define whether to use Bulk API for the job when the number of records in a job exceeds the limit you set.
     Once the Bulk API is enabled, configure the following settings:
     - **Batch limit** – Enter a percentage for the field. The maximum number of Bulk API batches that can be submitted per rolling 24-hour period is 15,000. If the usage of Bulk API in a backup exceeds the configured percentage of 15,000, IBM® Storage Protect for Cloud Salesforce will automatically switch to using Bulk API 2.0 (if enabled) and SOAP API for backup. The default value is 80%.
     - **Define scope** – The following options are provided:
       - **Backup and archive** – Enable Bulk API for backup and archive jobs.
       - **Restore** – Enable Bulk API for restore and sandbox seeding jobs. Note that the Bulk API is not supported when restoring metadata, fields, or archived data.
   - **Enable Bulk API 2.0 for backup** – Turn on/off the toggle to define whether to use Bulk API 2.0 for backup when the number of records in a backup job exceeds the limit you set.
     Once the Bulk API 2.0 is enabled, configure the following settings:
     - **Limit on query job number per backup** – Enter a percentage for the field. The maximum number of query jobs that can be submitted per 24-hour rolling window is 10,000. If the usage of Bulk API 2.0 in a backup exceeds the configured percentage of 10,000, IBM® Storage Protect for Cloud Salesforce will automatically switch to using the SOAP API for backup. The default value is 80%.

- **Limit on query result size per backup** – Enter a value for the field. The default value is 800 GB. The maximum size of query results that can be generated per 24 hour rolling window is 1000 GB. If the usage of Bulk API 2.0 in a backup exceeds the configured limit, IBM® Storage Protect for Cloud Salesforce will automatically switch to using the SOAP API for backup.

6. Click **Save** apply the settings.

Data Management

Data Cleanup

To comply with GDPR, IBM® Storage Protect for Cloud Salesforce provides the **Data Cleanup** feature to allow administrators to clear or overwrite the field values of backup records. Administrators can configure data cleanup templates to define the fields you want to clean up for each object. Note that audit fields are not supported by this function. For the supported and unsupported fields in data cleanup, refer to “Appendix E - Supported and Unsupported Fields in Data Anonymization and Cleanup” on page 125.

Any field values that can be empty in Salesforce will be cleared. For required fields, if they are related to other objects, or there is no need to overwrite, the original values will be kept; other required field values will be overwritten. Refer to the **How will field values be overwritten?** table for details.

To avoid accidental data loss, you can set an approval process for the data cleanup. With this feature enabled, data cleanup needs approval from administrators. For details, refer to Enable Approval Process for Data Cleanup.

How will field values be overwritten?

Field	Action	Overwritten Value	Example
Auto Number	Keep original value	/	/
Checkbox	Keep original value	/	/
Currency	Overwrite	Random number according to the character length and decimal precision limits of this field in Salesforce.	8888.00 – 965289.27
Date	Overwrite	The day when the data cleanup job is run for the field.	
Date/Time	Overwrite	The time when the data cleanup job is run for the field.	
Email	Overwrite	Random string + **@GDPR.com**.	user@contoso.com – abcd@GDPR.com
External Lookup Relationship	Related to other objects; Keep original value	/	/
Formula	Keep original value	/	/
Geolocation	Overwrite	Random latitude and longitude	
Lookup Relationship	Related to other objects; Keep the original value	/	/
Number	Overwrite	Random number according to the character length and decimal precision limits of this field in Salesforce.	123.45 – 159.35
Percent	Overwrite	Random percentage	
Phone	Overwrite	Random number. The character length is the same as the original value.	1234567890 – 1593574562
Picklist	Unsupported	/	/
Picklist (Multi-select)	Unsupported	/	/
Roll-Up Summary	Keep original value	/	/

Field	Action	Overwritten Value	Example
Text	Overwrite	**GDPR** + random string. If the length is shorter than 4 characters, generate a random string with the same character length.	contoso.com – GDPRasdf1Gh Ada – xHt
Text Area			
Text Area (Long)			
Text Area (Rich)			
Text (Encrypted)			
Time	Overwrite	The time when the data cleanup job is run for the field.	
URL	Overwrite	**http://GDPR.** + random string	http://contoso.com – http://GDPR.abcd1e

Enable Approval Process for Data Cleanup

To avoid accidental data loss, you can set an approval process for the data cleanup. With this feature enabled, data cleanup requests and email notifications will be sent to the administrators when you perform data cleanup.

Then administrators can access the IBM® Storage Protect for Cloud Salesforce interface and click **My tasks** (📅) on the upper-right of the interface to view the request details, and then approve or reject your requests. The deletion cleanup jobs will start when the requests are approved. Note that the requests will be automatically invalidated if not approved within 7 days.

Complete the following steps to enable the approval process for data cleanup:

- Navigate to **Settings** >**General**.
- Click the **Data cleanup** tab. All organizations that you manage are displayed.
- Turn on the toggle next to the organization for which you want to enable the approval process. Note that once enabled, the approval process cannot be disabled.
- In the **Enable approval process for data cleanup?** window, click **Enable** to confirm and enable the setting. You can also click **Cancel** to close the panel without saving any changes.

Configure a Data Cleanup Profile

Data cleanup profiles can help you to configure which fields you want to clean up for different objects.

Procedure

Complete the following steps to configure a data cleanup profile:

1. Navigate to **Settings** > **Profile management**.
2. Click the **Data cleanup profile** tab.
3. Click **Create profile**. The **Create a data cleanup profile** panel appears.
4. Select an object from the drop-down list.
5. Select the fields you want to clean up for the selected object by selecting the corresponding checkboxes.
6. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving the configurations. After you add data cleanup profiles, you can perform the following actions to manage the profiles:
    - View – Click the object name link in the **Object** column to view the cleanup fields for the object.
    - Edit – Click **Edit** to select and edit the object and fields.
    - Delete – Select the profiles and click **Delete** to delete the profiles.

Perform a Data Cleanup

Procedure

To clean up the field values of records, complete the following steps:

1. Navigate to **Data management › Data Cleanup**. All organizations that you manage are displayed.
2. Click **Clean up** next to the organization you want to clean up.
3. There are two ways to define the records whose field values you want to clean up.
   - **Search by keyword**
     - Select the objects from the **Objects** drop-down list.
     - In the **Keyword** field, select to search records by **Record name** or **Record ID**, and then enter a keyword in the search box. Click **Search** to search for the records whose names or IDs contain the keyword. The default search condition is to search the backup data within the last backup cycle.

       > **Note:** The IBM® Storage Protect for Cloud Salesforce system utilizes Salesforce Object Query Language (SOQL) and Salesforce Object Search Language (SOSL) to search records. Therefore, the keyword must meet the SOSL Search Query requirements.

       > **Note:** The wildcards are supported in the keywords of record names.

     - Select the records in the search results.
   - **Import a CSV file**
     - You can click **Download CSV template** to download the CSV template file for configuring record information.
     - Enter the object type API name in the **Object API Name** column, and enter the record ID in the **RecordId** column of each row.

     For standard objects, you can also refer to the Salesforce SOAP API to find the API name of the objects. For custom objects, you can navigate to **Setup** in your Salesforce environment to find the custom object and get the API name.

     - Click **Upload** to import the CSV file with record information configured.
   - Define field-level scope
     a. Click **Add object**.

     b. Select the object from the **Object** drop-down list.

     c. You can either add all the records of the object or filter the records for cleanup by following the steps below:
        - To add all records of the selected object, click **Save** directly.
        - To filter the records for cleanup, click **Add condition**. Select a field of the object and an operator, and then enter a value for the filter.

          You can click the Add (+) icon next to the condition and repeat the steps above to add more conditions.

          You can configure conditions using **And** or **Or**. With **And**, all conditions must be met; with **Or**, any one of the conditions can be met.
   - Click **Save** to apply the conditions.
4. Click **Next**.
5. In the **Select field scope** field, all objects you configured are listed in the table together with the number of records in each object. You can select the field scope to define the fields you want to cleanse for the records in each object.

   a. Select **All fields** – All fields will be cleaned up.

    b. Select a scope– Only the fields selected in the template will be cleaned up. You can click **View field scope** to preview the fields that will be cleaned up for this object. If there is no pre-configured profile for the object, select **Create profile** to add one. Refer to “Configure a Data Cleanup Profile” on page 60 to see how to create a profile.

6. In the **Do you want to export the original field values of records from the last backup job?** field, select if you want to export the original field values from the last backup.
7. In the **Enable scheduled cleanup** field, turn on the toggle and set the interval to enable scheduled cleanup for the organization.

> **Note:** You can update the interval or disable the scheduled cleanup later by clicking the scheduled cleanup tag for the required organization in **Data management** > **Data cleanup**.

8. Click **Clean up** to run the data cleanup job based on your configurations.
   If you have selected to export the original field values, you can download CSV data in the **Job monitor** when the job is finished.

Reporting

View API Usage Report

Navigate to **Reporting › API usage** to view the API usage report of organizations under the corresponding tabs.

The **API Usage** chart displays the percentage of the API usage limit by including both running and completed backup jobs in IBM® Storage Protect for Cloud Salesforce as well as the API usage limit percentage of the organization in the last 7 days. To maintain optimum performance and ensure that the Force.com API is available to all Salesforce customers, Salesforce balances transaction loads by imposing Total API Request Limits per 24 hours. When a call exceeds a request limit, an error is returned. The chart can provide you with a convenient way to check the condition of API usage. If a call exceeds the request limit, the backup or restore job will pause. IBM® Storage Protect for Cloud Salesforce will keep the progress and enquire Salesforce every 30 minutes. When there is an abundant API quota, IBM® Storage Protect for Cloud Salesforce will resume the progress to finish the job.

Administrators can also configure a percentage for the Salesforce API usage limit by clicking **Configure API usage limit** in the upper-right corner. In the panel, enter an integer from 1 to 100 to define the percentage. Make sure you set an appropriate value to ensure your jobs will not be affected. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving the configurations.

The total number of API requests allowed by Salesforce is defined by the users' licenses in the organization. For details, refer to the Salesforce documentation: API Request Limits and Allocations. For your current API usage, navigate to Salesforce > **System Overview** > **API Usage**.

If you have enabled Bulk API and Bulk API 2.0 for organizations, you can also view the percentage of Bulk API and Bulk API 2.0 usage limit on this page. To configure the limit, click **Configure Bulk API usage** in the chart. For details on the settings, refer to Configure Bulk API Usage.

Use Unusual Activities Analysis Report

IBM® Storage Protect for Cloud Salesforce will learn from your backup statistics and warn you of the organizations with unusual activities or that are under a potential ransomware attack.

Unusual activities are designed to provide visibility about atypical patterns within your environment, distinct from regular usage patterns. The unusual activities could be related to malware that is related to ransomware or non-ransomware. But in most cases they can be legitimate operations. It might be normal for a user to make changes that do not match their day-to-day patterns. While you should be aware that these changes are happening, you likely do not have to respond to every unusual activity report.

However, a potential ransomware attack is much more serious and requires your immediate attention. It refers to the real suspicious files that were detected in an organization that requires investigation.

To learn how you use your environment and build the pattern, the **Salesforce Unusual Activities Analysis** report requires at least 12 days of successful backups. Once any unusual activity or potential ransomware attack has been detected, you will receive an email notification. To enable the alert, refer to"Configure Notifications" on page 55 .

View the Report

The **Dashboard** tab displays the number of organizations protected by IBM® Storage Protect for Cloud and the number of organizations with unusual activities. The main chart in the **Dashboard** tab shows the data tracked over the last 30 days for unusual activities and potential ransomware attacks.

You can click the number to view the organizations with unusual activities or click the point on the chart to view the details of that specific date. The **Details** tab will show more information on the unusual activities and suspicious files for the reported organizations. You can download the report in an Excel file.

You can also go to the **Details** page directly to view the data in a table. You can adjust the time range to change the data scope or click an organization to view the report with its own details.

When you view the details of a specific organization, you can also adjust the time range to change the data scope and click a point in the chart to view the details of that date. The details are displayed below the chart.

You can download a report of all files with unusual activities in the organization for record or for further investigation.

Recover Suspicious Files to a Healthy State

To recover suspicious files to a safe state, click the **Restore suspicious files** button on the details pane of an organization. Then find a safe date and select the proper recovery point to restore.

The Recovery Point calendar will display a yellow dot under the date where its recovery points are detected with unusual activities. For details on the common restore settings, refer to Restore Backup Data.

> **Note:** To recover suspicious files of **ContentVersion** to a healthy state successfully, go to Salesforce and delete corresponding suspicious files first for the following reasons:
>
> - If the suspicious file in the Salesforce environment is a new version of the file before the ransomware attack, the file in the restore job will be skipped.
> - If the suspicious file in the Salesforce environment is a new file whose name is the same to the file before the ransomware attack, there will be two files with the same name in the Salesforce environment after the restore.

View the Subscription Consumption Report

Navigate to **Report Center › Subscription consumption** to view the consumption report of your IBM® Storage Protect for Cloud Salesforce subscription. If you have a trial subscription, a sample report is displayed.

In the **Subscription information** section, you can view the number of purchased user seats, consumed user seats, and available user seats, as well as the expiration date of your subscription.

In the **Subscription usage** section, you can view the number and percentage of consumed user seats by each organization. Click **Download** to download a report to view the charged license types and the number of users.

Job Monitor

The **Job monitor** page displays the operations that have taken place in IBM® Storage Protect for Cloud Salesforce.

About this task

- **Backup** – The backup job.
- **Restore** – The restore or pre-restore job.
- **Compare** – The compare objects or compare metadata job.
- **Backup export** – The backup data export job that is run by clicking **Export records** or **Export files** of a backup job in the job monitor. Note that there is a monthly limit (100 GB) on the capacity of files that can be exported.
- **On-demand export** – The backup data export job that is run by clicking **Export** while restoring records. Note that there is a monthly limit (100 GB) on the capacity of files that can be exported.
- **Auto-export** – The automatic export job of backup data based on the scheduled export policy.
- **Audit log auto-export** – The automatic export job of audit logs based on the scheduled export policy.
- **Data Cleanup** – The data cleanup job to clean up field values of records.
- **Sandbox seeding** – The sandbox seeding or pre-seeding job.
- **Discover** – The discover job.
- **Data service** – The data service job.
- **Retention**– The archived data retention job.

Procedure

You can perform the following actions on the job records:

- Use the search box to search for the records by job ID.
- Click **Filters** to filter the records by **Data range**, **Level**, **Type**, **Status** and **Organization**.
- Click **Columns** to choose the columns you want to display on this page.
- Click the Refresh data (↻) button to refresh the records.
- Select the **Only show jobs with data exported** checkbox to view the jobs for which the data has been exported to download data.
- Click the Job ID link of a record to view the job details. Refer to View Job Details for details..
- Hover your mouse over a record, click the More (•••) commands button and select an action if necessary:
    - **Download report** – Download a job report that contains the summary of the job information and details about the job. We are implementing error codes into job reports as a self-service approach for troubleshooting. Clicking the error code link in the downloaded job report will open the Troubleshooting Guide.
    - **Export records** – Export detailed backup data in a backup job to CSV files or MySQL files. In the **Export records** panel, select whether to export detailed backup data to CSV files or MySQL files, and whether you want to export the changed records after the last backup job or export all backup data in the current cycle. Then click **Export**. An export job will be added to the job queue, and you can view the progress of the job in the job monitor.
        - By default, the export capacity limit for your tenant is 100 GB per month.
        - You cannot start an export job when there is an existing export job running for the same organization.

    - By default, ContentVersion objects are exported with their parent ContentDocument. If the export capacity limit for this month is reached, the export of the latest ContentVersion will be skipped. However, the export of ContentDocument will continue. If this is an urgent issue, you can contact the IBM Software Support team for assistance.

- **Export files** – Export files of the protected objects. In the prompted window, select the objects for which you would like to export files, and whether you want to export the changed data after the last backup job or export all backup data in the current cycle, and then click **Export**. Only the following object types are supported: **Attachment**, **Document**, **Static Resource**, **Mailmerge Template**, and **Content Version**. An export job will be added to the job queue, and you can view the progress of the job in the job monitor. Note that there is a monthly limit (100 GB) on the capacity of files that can be exported.

- **Export metadata** – Export metadata in a backup job into a ZIP file.

  > **Note:** Several built-in Salesforce profiles do not have the same name when they are exported. If you create a custom profile with the same name as the exported name of the built-in Salesforce profile, the custom profile will overwrite the built-in profile. To avoid overwriting the built-in Salesforce profiles, refer to Appendix C - Exported Profile Names for Built-in Salesforce Profiles before naming a custom profile.

- **Download data** – Download and save the CSV files or MySQL files to a local location after any export job is completed. Files exceeding 50 GB will be divided into multiple smaller files. You can then download each of these files individually.

  > **Note:** When you use IBM® Storage Protect for Cloud default storage, the exported data can be retained for 7 days. If you want to download data, make sure you download it within 7 days after the export job is completed.

- **Rerun** – Rerun the restore, export, discover, and data cleanup jobs. If you rerun a restore job, all data will be restored again.
  Note the following:
    - Only failed, finished with an exception, skipped, and stopped jobs can be rerun.
    - Backup jobs cannot be rerun.

- **Stop** – Stop an in progress job.

  > **Note:** Backup and discover cannot be stopped.

View Job Details

Procedure

On the **Job details** page, you can view the settings of the job, or the data details in the job. For backup jobs in progress, successful and failed backup items during the backup are provided. You can also perform the following actions to manage the job:

- Click **Download report** to download a job report that contains the summary of the job information and details about the job. For failed or skipped restore job, you can get the **Old Record ID** in the job report. We are implementing error codes into job reports as a self-service approach for troubleshooting. Clicking the error code link in the downloaded job report will open the Troubleshooting Guide.
  By default, only failed records with exceptions are included in the detailed job report for restore jobs. If you need to view successful and skipped records, please contact IBM Software Support for assistance.

- For a backup job, you can view the **General Information** and backup details of data and metadata.
    - Under the **Data** tab, you can click **Filters** to filter the objects by object type or number range of removed/changed/added records. You can **Export records** or **Export files** of the protected objects.

To export records, select the objects that you want to export and click **Export records**. In the **Export records** panel, select whether to export detailed backup data to CSV files or MySQL files, and whether you want to export the changed data after the last backup job or export all backup data in the current cycle. Then click **Export**.

To export files, click **Export files** first. In the **Export files** window, select the objects for which you would like to export files, and whether you want to export the changed data after the last backup job or export all backup data in the current cycle, and then click **Export**. Only the following object types are supported: **Attachment**, **Document**, **Static Resource**, **MailmergeTemplate**, and **Content Version**.

An export job will be added to the job queue, and you can view the progress of the job in the job monitor.

> **Note:** You cannot start an export job when there is an existing export job running for the same organization. There is a monthly limit (100 GB) on the capacity of files that can be exported, and the exported data is only available for 7 days.

Click the **Compare** link to go to the **Compare objects** feature if you want to view the details of the deleted, changed, and added data with the last backup job. After the comparison, you can click the number link to view details and restore the deleted or changed records from the old backup job to the current organization by clicking the (↺) button next to the number.

- Under the **Metadata** tab, you can use the search box to search for metadata by metadata type. Click **Export metadata** to export metadata into a ZIP file.

> **Note:** Several built-in Salesforce profiles do not have the same name when they are exported. If you create a custom profile with the same name as the exported name of the built-in Salesforce profile, the custom profile will overwrite the built-in profile. To avoid overwriting the built-in Salesforce profiles, refer to "Appendix C - Exported Profile Names for Built-in Salesforce Profiles" on page 124 before naming a custom profile.

- For a restore job, you can view the **General Information** of the job, including the **Recovery point**, **Duration**, **Operator**, **Restore level**, and **Number of APIs used**.
- For a discover job, you can view the **General Information** and discover results. Only objects for which you have permission are listed in the discover report. In **General information**, you can click the **Object** link to list the objects searching from. You can also click **Filters** to filter the discovered records by object type. To preview the record, click the Record ID. The record details and related records are provided.
  To take actions to the discovered records, select the records you desired. You can select the checkbox next to the **Record ID** to select all available records, or select the checkbox next to an object to select all available records of the object. To restore the selected records, click **Restore** to jump to the restore steps. For details to restore records, refer to Restore Records. Then you can take the following actions:
  - **Compare** – To compare the backup data of the selected records with the current Salesforce data., click **Compare** to start the compare process. After the compare job has started, you can go to the job monitor to track the progress. After the job is finished, you can click the Job ID link to view the compare result.
  - **Restore** – To restore the selected records, click **Restore** to jump to the restore steps. For details to restore records, refer to Restore Records.
  - **Data cleanup** – To clear the field values of the selected records, click Data cleanup to jump to the cleanup steps. For details on data cleanup, refer to Data Cleanup.
  - **Export** – To export the selected backup records to CSV files or MySQL files, click **Export**. If you select the records of the following object types: **Attachment**, **Document**, **Static Resource**, **Mail Merge Template**, **Event Log File** and **Content Version**, you can select to export **Records** only or export **Records and files** of the objects. Note that the MySQL file format only supports exporting records, and any files will keep their original formats. The export job may take a long time depending on the number of records or selected time range, and it may slow down other running jobs. There is a monthly limit (100 GB) on the capacity of files that can be exported.

- For a data export or audit log export job, click the **Download export data** link to download and save the CSV files or MySQL files to a local location after the job completes. To obtain the password of the downloaded files, click the **Show password** button. Files exceeding 50 GB will be divided into multiple smaller files. You can then download each of these files individually.

  > **Note:** When you use IBM® Storage Protect for Cloud default storage, the exported data can be retained for 7 days. If you want to download data, make sure you download it within 7 days after the export job is completed.

- For a compare objects job, you can view the total number of records and the number of deleted, changed, and added records. Click **Filters** to filter the objects by object type or number range of removed/changed/added records.
  - Click the number link of the deleted records to view the detailed information about the deleted records on the **Delete details** page. You can click **Download** on the **Delete details** page to download a ZIP file to view the information about the deleted records.
  - Click the number link of the changed records to view the detailed information about the changed records on the **Change details** page. You can click **Download** on the **Change details** page to download a ZIP file to view the information about the changed records. Select the **Only show changed fields** checkbox to only view the fields that have been changed.
  - Click the number link of the added records to view the detailed information about the added records on the **Add details** page. You can also click **Download** on the **Add details** page to download a ZIP file to view the information about the added records.

  If you have the **Restore metadata** permission, you can also restore the deleted or changed metadata from the old backup job to the current organization by clicking the Restore (↺) button next to the number.

- For a compare metadata job, you can view the total number of metadata and the number of deleted, changed, and added metadata. Click **Filters** to filter the records by metadata type or number range of removed/changed/added metadata.
  - Click the **Download** (⤓) button next to the number of the deleted or added metadata to download a ZIP file to view the detailed information about the deleted or added metadata.
  - Click the number link of the changed metadata to view detailed information about the metadata.
    If you have the **Restore metadata** permission, you can also restore the deleted or changed metadata from the old backup job to the current organization by clicking the Restore (↺) button next to the number.

- For a pre-restore or pre-seeding job, you can view the **General Information** and review job recommendations. You can adjust the settings directly in this page.
  When ready, click **Start restore/seeding** on the upper right corner of the page to execute the actual restore/seeding and the settings you just adjusted will apply to the actual restore/seeding. For pre-seeding jobs, the changes you made on this page will also apply to this sandbox seeding template when you start the sandbox seeding job.

  In the page, four sections of recommendations are provided:
  - **Ensure there is sufficient storage available in the destination organization** – The objects included in the job are listed in the table together with the number of records in each object, and the estimated size of the data is provided. If the storage available in the destination organization is insufficient, you can either delete some existing data in the destination organization or increase the storage limit to provide enough storage for the restore or seeding.
  - **Deactivate related automations temporarily** – IBM® Storage Protect for Cloud Salesforce will check related triggers, flows and processes , workflow rules and validation rules in the destination environment, and display them in this section.
    To customize the deactivation scope, you can click **Deactivate** and define the deactivation scope to deactivate related automations temporarily:
    - **All related automations** – All the related automations will be deactivated during the restore.
    - **Custom deactivation scope** – Select the automations you want to deactivate during the restore.

Note that the settings do not apply to third-party automations.

You can review the current deactivation scope by clicking **Temporarily deactivated automations**. To remove an automation from the scope, click More commands (•••) button next to the automation in the panel, then click **Remove**.

  - **Grant Edit and Create permissions for the following objects** – The account that connect the Salesforce organization in IBM® Storage Protect for Cloud does not have Edit and Create permissions to objects listed in this section. To successfully restore or seed the objects, grant the Edit and Create permissions to the objects in your Salesforce environment.
  - **Missing Edit permission for the following fields** – The account that connect the Salesforce organization in IBM® Storage Protect for Cloud lacks Edit permission for the fields listed in this section. To correctly restore or seed the corresponding field values, grant Edit permission for these fields in Salesforce. Otherwise, the field values will be blank after the restore or seeding.
  - **Address duplicate rules in the Salesforce environment** – Active duplication rules in the Salesforce environment are listed in this section. They are designed to prevent the creation of duplicate data. To address duplicate rules, refer to the Troubleshooting Guide.
  - **Identify the missing required parent objects in the Salesforce environment** – For the objects in the **Base object** column, their required parent object records do not exist in the Salesforce environment. To resolve the issue, click **Configure** on the upper right corner of the section, and select the required parent objects to restore them together.

- For a data service job, you can view the **General Information**. In **General information**, you can click the **Object** link to list the objects included in the data service job.

Monitor Alerts

IBM® Storage Protect for Cloud Salesforce can send email alerts for monitoring data and metadata changes between backups. Administrators can configure the alert rules to an organization. When the alert of the organization is enabled and any of the rules are met, email alerts will be sent to the configured users and the user who registered the organization in IBM® Storage Protect for Cloud.

Before you begin

Before you configure the alert rules, make sure at least one backup job has been completed for the organization to load the backup objects.

Procedure

Complete the following steps to configure the alert rules:

1. Navigate to **Activity › Monitor alerts**.
2. Click **Data alert** or **Metadata alert** to monitor data or metadata changes. The **Data alert** page appears and all organizations that you manage are displayed
3. Turn on the toggle next to an organization you want to enable the alerts.
4. Click **Add** to add a rule.
5. Configure the object, operation, condition, and number of records for the rule. You can select multiple conditions for a single object or metadata type.
   For example: The rule is configured as **Account; Add; >=; 5**. When there are five or more newly added records in the backup job compared with the last backup, email alerts will be sent.

   To configure the record scope of an object, click **Edit** in the Record scope column, and follow the steps to add field-level conditions to filter the records:

   a. Click **Add condition**.

   b. Select a field of the object and then select an operator.

   c. Enter a value for the filter.

   d. Click the Add icon next to the condition and repeat the steps above to add more conditions. You can configure conditions using **And** or **Or**. With **And**, all conditions must be met; with **Or**, any one of the conditions can be met.

   e. Click **Save** to apply the conditions.

   > **Note:** If the operation for the rule is **Remove**, the field-level filter cannot be applied to the object.

   If you want to delete a rule, click the delete (🗑) button of the rule.
6. In the **Send email notifications to the following email addresses** text box, enter the usernames of users who will receive the email notifications.
7. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving these configurations.
   On the **Data alert** and **Metadata alert** page, you can turn on/off the toggle next to an organization to enable or disable the alerts

Data Export

IBM® Storage Protect for Cloud Salesforce allows administrators to export backup data or audit logs within a defined data range or based on a schedule. For data export, records are categorized and stored in separate based on their respective objects.

Scheduled Data Export

Administrators can complete the following steps to configure a policy for scheduled data export:

1. Navigate to **Data management** > **Data export**.

2. Select **Scheduled data export**. All organizations that you manage are displayed.

3. Turn on the toggle next to the organization you want to enable the scheduled data export for and the **Configure scheduled data export policy** panel appears.

   For an organization with a scheduled data export policy, you can click the edit (✏) icon in the **Action** column to edit the policy, or turn off the toggle next to organization to disable the scheduled data export.

4. Select objects you want to export by selecting the corresponding checkboxes from the **Export objects** drop-down list.

5. For **Record scope**, select whether to export all records that have been backed up in the current backup cycle, or only the records that were backed up since the last export job.

6. Enter the maximum number of items in each exported CSV file in the **Maximum item number per CSV file** field.

7. In the **Export frequency** section, configure the following settings:

   - **Start time** – Select the start time of the schedule, and the first export job will be automatically performed at that start time.

     > **Note:** If a user logs into the IBM® Storage Protect for Cloud Salesforce service from a time zone that is not where the export schedule is configured, the start time of the export job will be converted to the local time of that time zone where the user logged in.

   - **Interval** – Configure the interval for the scheduled export jobs.

8. In the **Export to** section, select the storage type you want to use and configure the settings. The **Microsoft Azure Storage**, **SFTP**, **Amazon S3**, **Amazon S3-Compatible Storage**, **IBM Cloud Object Storage**, and **IBM Storage Protect - S3** types are supported. For detailed settings for different storage types, refer to "Configure a Custom Storage Location and Database" on page 46.

9. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving these configurations.

One-time data export

Administrators can complete the following steps to export specific backup data within a defined date range:

1. Navigate to **Data management** > **Data export**.

2. Select **One-time data export**.

3. Select an organization from which you want to export data.

4. Select objects you want to export by selecting the corresponding checkboxes from the **Export objects** drop-down list.

5. Select the date range for the data you want to export.

6. Select the file format for the export. Note that the MySQL file format only supports exporting records, and any files will keep their original formats.

7. If you select the following object types: **Attachment**, **Document**, **Static Resource**, **Mail Merge Template**, **Event Log File** and **Content Version**, you can select to export **Records** only or export **Records and files** of the objects. There is a monthly limit (100 GB) on the capacity of files that can be exported.

8. Click **Export**. The export job may take a long time depending on the number of records or selected time range, and it may slow down other running jobs. And the exported data is only available for 7 days.

Scheduled audit log export

For organizations that have enabled audit log backup, administrators can complete the following steps to configure a policy for scheduled audit log export:

1. Navigate to **Data management** > **Data export**.

2. Select **Scheduled audit log export**. All organizations that have enabled audit log backup are displayed.

3. Turn on the toggle next to the organization you desired to enable the scheduled audit log export and the **Configure scheduled audit log export policy** panel appears.

4. Select the types of audit logs you want to export by selecting the corresponding checkboxes from the **Audit log types** drop-down list.

5. For **Audit log scope**, select whether to export all audit logs that have been backed up in current backup cycle, or only the audit logs that have been backed up in the current backup cycle.

6. Enter the maximum number of items in each exported CSV file in the **Maximum item number per CSV file** field.

7. In the **Export frequency** section, configure the following settings:

   - **Start time** – Select the start time of the schedule, and the first export job will be automatically performed at that start time.

     > **Note:** If a user logs into the IBM® Storage Protect for Cloud Salesforce service from a time zone that is not the one where the export schedule is configured, the start time of the export job will be converted to the local time of that time zone where the user logged in.

   - **Interval** – Configure the interval for the scheduled export jobs.

8. In the **Export to** section, select the storage type you want to use and configure the settings. The **Microsoft Azure Storage**, **SFTP**, **Amazon S3**, **Amazon S3-Compatible Storage**, **IBM Cloud Object Storage**, and **IBM Storage Protect - S3** types are supported. For the detailed settings of different storage types, refer to Configure a Custom Storage Location and Database.

9. Click **Save** to save the configurations, or click **Cancel** to close the panel without saving these configurations.

One-time audit log export

Administrators can complete the following steps to export specific audit logs generated within a defined date range:

1. Navigate to **Data management** > **Data export**.

2. Select **One-time audit log export**.

3. Select an organization from which you want to export data.

4. Select the types of audit logs you want to export by selecting the corresponding checkboxes from the **Audit log types** drop-down list.

5. Select the date range for the data you want to export.

6. Click **Export**. There is a monthly limit (100 GB) on the capacity of audit logs that can be exported. And the exported data is only available for 7 days.

System Auditor

Click **System auditor** in the left navigation to view the user activities in IBM® Storage Protect for Cloud Salesforce. You can click the bold Time of the user activities to change details.

You can perform the following actions on the records of user activities:

- Click **Filters** to filter the **Organization**, **Data range**, and **Operation component**. Select the conditions and then click **Apply** to filter the records.
- Use the search box to search for the activities by username.
- Click the Refresh (🔄) button to refresh the records.
- Export the audit records by following the steps below:

  a. Click the Export (📤) button. The **Export audit report** window appears.

  b. You can select the date range within 1 year for the export.

  c. Click **Export**. The audit report will be exported to your browser's download location.

Subscription

Click **Subscription** in the left navigation to view the consumption report of your IBM® Storage Protect for Cloud Salesforce subscription for **Salesforce backup**. If you have a trial subscription, a sample report is displayed

In the **Subscription information** section, you can view the number of purchased user seats, consumed user seats, and available user seats, as well as the expiration date of your subscription.

In the **Subscription usage** section, you can view the number and percentage of consumed user seats by each organization. Click **Download** to download a report to view the charged license types and the number of users.

View Subscription Notifications

You can view notifications of your subscription in the **Notifications** menu by clicking the bell (🔔) button.

In the menu, you can view the number of assigned user seats and the number of purchased user seats. When you click the **Assigned** tile, you can also click the **subscription report** link to view more details of your subscription.

Troubleshooting Guide

The troubleshooting guide is aimed at addressing unexpected issues and errors that you may encounter when using IBM® Storage Protect for Cloud Salesforce.

DuplicateName

Issue:

Some records encountered exceptions in the restore with the following error code:

- **DuplicateName**

Details:

Salesforce does not allow duplicate names for records within the same object. The name of the record you are trying to restore conflicts with existing records in the Salesforce environment.

Solution:

To resolve this error due to duplicate records in the Salesforce environment, consider renaming the record with the duplicate name. If the existing record is no longer needed, you can delete it.

For sandbox seeding, you can configure sandbox seeding settings in IBM® Storage Protect for Cloud Salesforceto delete the existing data of the specified objects from the sandbox before the seeding process.

DuplicateValue

Issue:

Some records encountered exceptions in the restore with the following error code:

- **DuplicateValue**

Details:

There are two possible reasons:

- The current configuration in the Salesforce environment may include active duplication rules designed to prevent the entry of duplicate data.
- The object may have unique fields that do not allow different records to have the same value.

Solution:

For the first reason, refer to the following scenarios:

- If the prevention of duplicate records aligns with your data management objectives, this message serves merely as a confirmation of the active rules. In this case, no further action is required, and any error messages regarding duplicates can be disregarded.
- If the enforcement of duplicate prevention rules does not fit your use case, you can manually deactivate these rules within your Salesforce environment.

For the second reason, you can uncheck the **Do not allow duplicate values** option for this field in the Salesforce environment.

FlowException

Issue:

Some records encountered exceptions in the restore with the following error code:

- **FlowException**

Details:

There is an active flow under the object in your Salesforce environment and the flow is a blocker to restore jobs.

Solution:

You can disable the corresponding flow in your Salesforce environment or enable the **Deactivate related triggers, flows, workflow rules, and processes during the restore** option when configuring restore settings in IBM® Storage Protect for Cloud Salesforce.

GlobalPicklistNotExist

Issue:

Some records encountered exceptions in the restore with the following error code:

- **GlobalPicklistNotExist**

Details:

The field of the records is a picklist.

If you restore the data to the original organization, the picklist field uses the values from a global picklist, but the global picklist does not exist in your Salesforce environment now.

If you restore the data to another organization, the picklist field uses the values from a global picklist in the source organization, but the global picklist does not exist in the destination organization.

The field name is provided in the **Comment** column of the job report.

Solution:

If you restore the data to the original organization, create the global picklist first in your Salesforce environment before the restore.

If you restore the data to another organization, create the global picklist first in the destination organization before the restore.

You can also create the global picklist by restoring metadata in IBM® Storage Protect for Cloud Salesforce. Follow the steps below:

1. Get the **Global Value Set** of the global picklist in the Salesforce environment.
2. Follow the steps in the User Guide to find the **Global Value Set** in IBM® Storage Protect for Cloud Salesforce and restore it to the Salesforce environment.

InsufficientAccess

Issue:

Some metadata or records of an object encountered exceptions in the backup/restore with the following error code:

- **InsufficientAccess**

Details:

In the backup, the error occurs due to insufficient access permissions.

In the restore, the error may be due to the object not being supported for creation or update in the Salesforce environment. Please verify this in the latest Salesforce documentation. If the object is allowed for creation and update, the issue occurs due to insufficient access permissions.

Solution:

If you encounter the error in the backup, please grant the **Modify Metadata Through Metadata API Functions/Modify All Data** permission to the authenticated user for the organization connection.

If you encounter the error in the restore, we recommend granting the **Modify All Data** permission to the authenticated user for the organization connection.

InsufficientAccessReferenceId

Issue:

Some records encountered exceptions in the restore with the following error code:

- **InsufficientAccessReferenceId**

Details:

The parent object records do not exist in the Salesforce environment.

Solution:

If you did not select the option to restore the parent object records, select it and rerun the restore job.

If you already selected this option, the exception may be due to the unsuccessful restore of the parent object records. Resolve the errors in the restore of the parent object records and rerun the restore job.

InvalidEmailAddress

Issue:

Some records encountered exceptions in the restore with the following error code:

- **InvalidEmailAddress**

Details:

Due to your email settings in the destination Salesforce environment, IBM® Storage Protect for Cloud Salesforce will validate the email address in the restore process. The email address is invalid.

Solution:

Follow the steps to update the settings in the destination Salesforce environment and perform the restore again.

1. Click your avatar in destination organization, then select **Settings** in the dropdown menu.
2. In the left sidebar, select **Email** > **My Email Settings**.
3. Select **Send through Salesforce**, and save the updates.

InvalidNamespace

Issue:

Some records of an object encountered exceptions in the restore with the following error code:

- **InvalidNamespace**

Details:

The records use a namespace that belongs to a third-party package. IBM® Storage Protect for Cloud Salesforce does not support the backup and restore of third-party packages.

InvalidRecordType

Issue:

Some records failed in the restore with the following error code:

- **InvalidRecordType**

Details:

The authenticated user for the organization connection lacks the necessary permissions for the current record type.

Solution:

Grant the permission of the record type to the authenticated user in Salesforce.

If the specified record type does not exist in your Salesforce environment, select to restore parent object records and rerun the restore job in the IBM® Storage Protect for Cloud Salesforce interface.

LookupFilterRule

Issue:

Some records of an object encountered exceptions in the restore with the following error code:

- **LookupFilterRule**

Details:

There is a lookup filter on the field of the object in your Salesforce environment and the lookup filter is a blocker to restore jobs. The field name is provided in the **Comment** column of the job report.

Solution:

You can manually deactivate the corresponding lookup filter in your Salesforce environment.

ManagedObject

Issue:

Some records encountered exceptions in the restore with the following error code:

- **ManagedObject**

Details:

Salesforce does not allow duplicate names for records within the same object. The name of the record you are trying to restore conflicts with existing records in the Salesforce environment.

Solution:

These records are generated from third-party apps. IBM® Storage Protect for Cloud Salesforce does not support restoring records associated with third-party apps,

MetadataMissingParent

Issue:

Some records encountered exceptions in the restore with the following error code:

- **MetadataMissingParent**

Details:

The required parent metadata has encountered exceptions in the restore process.

Solution:

Try to address the error on the parent metadata and perform the restore again.

MoreThanOneSender

Issue:

Some records encountered exceptions in the restore with the following error code:

- **MoreThanOneSender**

Details:

The sender address of the email conflicts with the predefined value set for the **From** field in the Salesforce environment.

Solution:

Follow the steps to delete the predefined value in Salesforce environment and perform the restore again:

- Go to Classic Salesforce > **Setup** > **Customize** > **Cases** > **Buttons, Links, and Actions**.

- Click **Email**.
- In the **Predefined Field Values** section, click **Del** to delete the predefined value configured for **From** field.

MissAuditFieldPermission

Issue:

Some records encountered exceptions in the restore with the following error code:

- **MissAuditFieldPermission**

Details:

The consent user for the app profile does not have sufficient permissions to create or update the following fields: CreatedDate, CreatedById, and LastModifiedById.

Solution:

If you encounter an error in the restore, please grant the **Set Audit Fields upon Record Creation** permission to the consent user for the app profile.

MissValueForPicklist

Issue:

Some records encountered exceptions in the restore with the following error code:

- **MissValueForPicklist**

Details:

The field of the records is a picklist.
If you restore the data to the original organization, some picklist values previously included in your Salesforce environment are not included now.

If you restore the data to another organization, some picklist values in the source organization are not included in the picklist field in the destination organization or there are no corresponding values in the destination organization.

The field name and the values are provided in the **Comment** column of the job report.

Solution:

If you restore the data to the original organization, check whether there are corresponding values in your Salesforce organization.

If you restore the data to another organization, check whether there are corresponding values in the destination organization.

If yes, you can add the missing values to the picklist field.

MultipleAccountsException

Issue:

Some records encountered exceptions in the restore with the following error code:

- **MultipleAccountsException**

Details:

The object is the **AccountContactRelation**. It represents a relationship between a contact and one or more accounts. The **Allow users to relate a contact to multiple accounts** setting is disabled in the Salesforce environment and limits the restore of such relationships.

Solution:

Enable the **Allow users to relate a contact to multiple accounts** setting in **Account Settings** in the Salesforce environment.

NoBackupData

Issue:

Some records encountered exceptions in the restore with the following error code:

- **NoBackupData**

Details:

The records might be the parent or child object records of other records, so they are included in the restore process. However, the records do not exist in our backup data.

There are two possible reasons:

- When creating the sandbox, data is copied from the production environment. It is likely that the data was not fully copied, and therefore, the records do not exist in the Salesforce environment and haven't been backed up.
- The authenticated user for the organization connection lacks the necessary permissions for this object, resulting in the records not being backed up.

Solution:

Please verify if the records exist in your Salesforce environment. If they exist, grant necessary permissions for the records and run a backup job.

NotEnabledForFeed

Issue:

Some records of an object encountered exceptions in the restore with the following error code:

- **NotEnabledForFeed**

Details:

The Feed Tracking was enabled for the object fields before the backup, but it was not enabled the corresponding object fields in the destination.

Solution:

Follow the steps to update the settings for the object in the destination Salesforce environment and perform the restore again.

1. Click **Setup** on the upper right corner of your destination organization, then search and select **Chatter**.
2. Click **Customize field tracking in your feeds**.
3. Select the corresponding object and enable feed tracking for its fields.

ObjectNotFound

Issue:

Some records of an object encountered exceptions in the archive with the following error code:

- **ObjectNotFound**

Details:

The associated object was deleted in Salesforce environment.

ReferenceConvertedLeadException

Issue:

Some records of an object encountered exceptions in the restore with the following error code:

- **ReferenceConvertedLeadException**

Details:

Salesforce does not allow duplicate names for records within the same object. The name of the record you are trying to restore conflicts with existing records in the Salesforce environment.

Solution:

The parent of the object is a converted lead object. IBM® Storage Protect for Cloud Salesforce do not support restoring records associated with converted lead objects.

RelationshipAlreadyExist

Issue:

Some metadata encountered exceptions in the restore with the following error code:

- **RelationshipAlreadyExist**

Details:

Salesforce does not allow duplicate child relationship names. The child relationship namesbetween the metadata you are trying to restore conflicts with existing child relationship names in the Salesforce environment.

Solution:

To resolve this error due to duplicate child relationship names in the Salesforce environment, consider renaming the child relationship with the duplicate name.

If the object or reference field has been deleted but not erased, erase the deleted object or reference field before running the restore job.

RequiredParentNotExist

Issue:

Some child object records encountered exceptions in the restore with the following error code:

- **RequiredParentNotExist**

Details:

The required parent object records do not exist in the Salesforce environment.

Solution:

If you did not select the option to restore the parent object records, select it and rerun the restore job.

If you already selected this option, the exception may be due to the unsuccessful restore of the parent object records. Resolve the errors in the restore of the parent object records and rerun the restore job.

StorageLimitExceeded

Issue:

Some records encountered exceptions in the restore with the following error code:

- **StorageLimitExceeded**

Details:

The storage of the destination organization has exceeded the limit and there is not enough storage for the restore.

Solution:

You can either delete some existing data in the destination organization or increase the storage limit to provide enough storage for the restore.

StringTooLong

Issue:

Some records encountered exceptions in the restore with the following error code:

- **StringTooLong**

Details:

The length of the field value in the backup data exceeds the length limit of the field in the destination Salesforce organization.

Solution:

Modify the length limit of the field in the destination Salesforce organization.

Third-PartyRulesOrValidation

Issue:

Some records encountered exceptions in the restore with the following error code:

- **Third-PartyRulesOrValidation**

Details:

There are active third-party automations (triggers, flows, workflow rules, processes, and validation rules) in your Salesforce environment that block restore jobs.

Solution:

IBM® Storage Protect for Cloud Salesforce does not support deactivating third-party automations. You can deactivate the corresponding triggers, flows, workflow rules, processes, and validation rules of the third-party apps in your Salesforce environment.

TriggerException

Issue:

Some records of an object encountered exceptions in the restore with the following error code:

- **TriggerException**

Details:

There is a trigger under the object in your Salesforce environment and the trigger is a blocker to restore jobs.

Solution:

You can disable the corresponding trigger in your Salesforce environment or enable the **Deactivate related triggers, flows, workflow rules, and processes during the restore** option when configuring restore settings in IBM® Storage Protect for Cloud Salesforce.

UnableToLockRow

Issue:

Some records encountered exceptions in the restore with the following error code:

- **UnableToLockRow**

Details:

The records are currently being accessed by a third-party API, rendering them unavailable for restoration through our API currently. For details, refer to the Salesforce article: Error 'Unable to lock row - Record currently unavailable'.

Solution:

The most appropriate action to resolve this issue is to attempt to rerun the restoration job later when the records may no longer be used by the third-party API.

UnsupportCreate

Issue:

Some records encountered exceptions in the restore with the following error code:

- **UnsupportCreate**

Details:

Due to Salesforce API limitations, it’s not supported to create this type of object or its fields in the Salesforce environment.

> **Note:** For the **EmailMessage** object, the creation is only supported when the email is in Draft status.

UnsupportUpdate

Issue:

Some records encountered exceptions in the restore with the following error code:

- **UnsupportUpdate**

Details:

Due to Salesforce API limitations, it’s not supported to update this type of object or its fields in the Salesforce environment.

> **Note:** Certain objects can only be updated when specific field values are met. If the field value does not satisfy these conditions, it may result in the error. For the field and its corresponding value, refer to the job report comment.

ValidationException

Issue:

Some records of an object encountered exceptions in the restore with the following error code:

- **ValidationException**

Details:

There is an active validation rule on the object in your Salesforce environment and the validation rule is a blocker to restore jobs.

Solution:

You can deactivate the corresponding validation rule in your Salesforce environment or enable the **Deactivate all validation rules during the restore** option when configuring restore settings in IBM® Storage Protect for Cloud Salesforce.

Appendices

The following table details the appendices included in this document:

Appendix	Description
"Appendix A - Permissions" on page 85	Lists the permissions available in IBM® Storage Protect for Cloud Salesforce.
"Appendix B - Supported and Unsupported Objects for Backup and Restore" on page 86	Lists the objects that are not supported by IBM® Storage Protect for Cloud Salesforce.
Appendix C - Exported Profile Names for Built-in Salesforce Profiles	Lists the profile names for built-in Salesforce profiles and their associated exported profile names.
"Appendix D - IBM Storage Protect for Cloud Salesforce Subscription Retention Information" on page 125	Details the subscription retention information.
Appendix E - Supported and Unsupported Fields in Data Anonymization and Cleanup	Lists the fields that are supported or not supported for data anonymization and cleanup in IBM® Storage Protect for Cloud Salesforce.
Appendix F - Supported and Unsupported Metadata Types for Backup and Restore	Lists the metadata types that are supported or not supported for backup and restore in IBM® Storage Protect for Cloud Salesforce.

Appendix A - Permissions

The table below displays the permissions available in IBM® Storage Protect for Cloud Salesforce.

Category	Permission	Definition
Backup	Back up now	The user with this permission can back up the data in the organization at any time, export backup data to CSV files, export metadata, and download a backup job report.
	Export data to CSV	The user with this permission can export backup data to CSV files, and download a backup job report.
	Export metadata	The user with this permission can export metadata to a ZIP file, and download a backup job report.
Export	Export data	The user with this permission can export backup data and download a backup/archive job report.
	Export metadata	The user with this permission can export metadata and download a backup job report.
Restore	Restore organization	The user with this permission can restore specific objects, restore records by importing CSV files, and download a restore job report.
	Restore objects	The user with this permission can restore the whole organization, including all objects and records, restore records by importing CSV files, and download a restore job report.

Category	Permission	Definition
	Restore records	The user with this permission can restore specific records, restore records by importing CSV files, and download a restore job report.
	Restore fields	The user with this permission can restore values of specific fields, restore records by importing CSV files, and download a restore job report.
	Restore metadata	The user with this permission can restore metadata and download a restore job report.
Sandbox Seeding	Manage sandbox seeding templates and run sandbox seeding jobs	The user with this permission can manage sandbox seeding templates, run sandbox seeding jobs, and download the sandbox seeding job report.
Compare	Compare data	The user with this permission can compare the objects and view the compare results.
	Compare metadata	The user with this permission can compare the metadata and view the compare results.
Discover	Discover data	The user with this permission can run global full-text search through backup records and view the discover results.

Appendix B - Supported and Unsupported Objects for Backup and Restore

Supported and Unsupported Objects for Backup and Restore

Some objects are not supported by IBM® Storage Protect for Cloud Salesforce due to Salesforce SOAP API limitations.

Refer to the following table to view the supported and unsupported objects in backup and restore. To learn more details about the Salesforce objects, see Salesforce SOAP API

Object Name	Support Status in Backup	Support Status in Restore	Comments
AcceptedEventRelation	Supported	Unsupported	
Account	Supported	Supported	
AccountBrand	Supported	Supported	
AccountBrandShare	Supported	Supported	
AccountChangeEvent	Unsupported	Unsupported	
AccountCleanInfo	Supported	Supported	
AccountContactRelation	Supported	Supported	
AccountContactRole	Supported	Supported	
AccountContactRoleChangeEvent	Unsupported	Unsupported	
AccountFeed	Supported	Supported	
AccountHistory	Unsupported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
AccountOwnerSharingRule	Unsupported	Unsupported	
AccountPartner	Supported	Unsupported	
AccountRelationship	Supported	Supported	
AccountRelationshipFeed	Supported	Unsupported	
AccountRelationshipHistory	Unsupported	Unsupported	
AccountRelationshipShare	Supported	Supported	
AccountRelationshipShareRule	Supported	Supported	
AccountShare	Supported	Supported	
AccountTag	Supported	Unsupported	
AccountTeamMember	Supported	Supported	
AccountTerritoryAssignmentRule	Unsupported	Unsupported	
AccountTerritoryAssignmentRuleItem	Unsupported	Unsupported	
AccountTerritorySharingRule	Unsupported	Unsupported	
AccountUserTerritory2View	Unsupported	Unsupported	
ActionLinkGroupTemplate	Supported	Supported	
ActionLinkTemplate	Supported	Supported	
ActionPlan	Supported	Supported	
ActionPlanItem	Supported	Supported	
ActionPlanTemplate	Supported	Supported	
ActionPlanTemplateItem	Supported	Supported	
ActionPlanTemplateItemValue	Supported	Supported	
ActionPlanTemplateVersion	Supported	Supported	
ActiveFeatureLicenseMetric	Supported	Unsupported	
ActivePermSetLicenseMetric	Supported	Unsupported	
ActiveProfileMetric	Supported	Unsupported	
ActiveScratchOrg	Supported	Supported	
ActiveScratchOrgFeed	Supported	Unsupported	
ActiveScratchOrgHistory	Unsupported	Unsupported	
Activity	Supported	Supported	
ActivityUserConnectionStatus	Unsupported	Unsupported	
ActivityHistory	Unsupported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
AdditionalUnsupportedNumber	Supported	Supported	
Address	Supported	Supported	
AggregateResult	Unsupported	Unsupported	
AIApplication	Supported	Unsupported	
AIApplicationConfig	Supported	Unsupported	
AIInsightAction	Supported	Unsupported	
AIInsightFeedback	Supported	Unsupported	
AIInsightReason	Supported	Unsupported	
AIInsightValue	Supported	Unsupported	
AIPredictionEvent	Unsupported	Unsupported	
AIRecordInsight	Supported	Unsupported	
AlternativePaymentMethod	Supported	Supported	
Announcement	Supported	Supported	
ApexClass	Supported	Unsupported	
ApexComponent	Supported	Supported	
ApexLog	Supported	Unsupported	
ApexPage	Supported	Supported	
ApexPageInfo	Unsupported	Unsupported	
ApexTestQueueItem	Supported	Unsupported	
ApexTestResult	Supported	Unsupported	
ApexTestResultLimits	Supported	Supported	
ApexTestRunResult	Supported	Supported	
ApexTestSuite	Supported	Supported	
ApexTrigger	Supported	Unsupported	
ApexTypeImplementor	Unsupported	Unsupported	
ApiEvent	Unsupported	Unsupported	
ApiEventStream	Unsupported	Unsupported	
AppAnalyticsQueryRequest	Supported	Supported	
AppDefinition	Supported	Unsupported	
AppExtension	Supported	Supported	
AppleDomainVerification	Supported	Unsupported	
AppMenuItem	Supported	Unsupported	
Approval	Supported	Unsupported	
AppTabMember	Supported	Unsupported	
AssessmentIndicatorDefinition	Supported	Supported	
AssessmentIndicatorDefinitionfeed	Supported	Unsupported	
AssessmentIndicatorDefinitionShare	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
AssessmentTask	Supported	Supported	
AssessmentTaskContentDocument	Supported	Supported	
AssessmentTaskDefinition	Supported	Supported	
AssessmentTaskDefinitionFeed	Supported	Unsupported	
AssessmentTaskDefinitionShare	Supported	Unsupported	
AssessmentTaskFeed	Supported	Unsupported	
AssessmentTaskIndDefinition	Supported	Supported	
AssessmentTaskIndDefinitionFeed	Supported	Unsupported	
AssessmentTaskOrder	Supported	Supported	
AssessmentTaskShare	Supported	Supported	
Asset	Supported	Supported	
AssetChangeEvent	Unsupported	Unsupported	
AssetDowntimePeriod	Supported	Supported	
AssetFeed	Supported	Unsupported	
AssetHistory	Unsupported	Unsupported	
AssetOwnerSharingRule	Unsupported	Unsupported	
AssetRelationship	Supported	Supported	
AssetRelationshipFeed	Supported	Unsupported	
AssetRelationshipHistory	Unsupported	Unsupported	
AssetShare	Supported	Unsupported	
AssetTag	Supported	Unsupported	
AssetTokenEvent	Unsupported	Unsupported	
AssetWarranty	Supported	Supported	
AssignedResource	Supported	Supported	
AssignmentRule	Supported	Unsupported	
AssociatedLocation	Supported	Supported	
AssociatedLocationHistory	Unsupported	Unsupported	
AsyncApexJob	Supported	Unsupported	
AsyncOperationEvent	Unsupported	Unsupported	
AsyncOperationStatus	Unsupported	Unsupported	
AttachedContentDocument	Unsupported	Unsupported	
AttachedContentUnsupportedNote	Unsupported	Unsupported	
Attachment	Supported	Supported	
Audience	Supported	Unsupported	
AuraDefinition	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
AuraDefinitionBundle	Supported	Supported	
AuraDefinitionBundleInfo	Unsupported	Unsupported	
AuraDefinitionInfo	Unsupported	Unsupported	
AuthConfig	Supported	Unsupported	
AuthConfigProviders	Supported	Unsupported	
AuthorizationForm	Supported	Supported	
AuthorizationFormConsent	Supported	Supported	
AuthorizationFormConsentChangeEvent	Unsupported	Unsupported	
AuthorizationFormConsentHistory	Unsupported	Unsupported	
AuthorizationFormDataUse	Supported	Supported	
AuthorizationFormDataUseHistory	Unsupported	Unsupported	
AuthorizationFormHistory	Unsupported	Unsupported	
AuthorizationFormShare	Supported	Unsupported	
AuthorizationFormText	Supported	Supported	
AuthorizationFormTextHistory	Unsupported	Unsupported	
AuthProvider	Supported	Supported	
AuthSession	Supported	Unsupported	
BackgroundOperation	Supported	Unsupported	
BackgroundOperationResult	Unsupported	Unsupported	
BatchApexErrorEvent	Unsupported	Unsupported	
BatchProcessJobDefView	Unsupported	Unsupported	
BrandTemplate	Supported	Supported	
BriefcaseAssignment	Supported	Unsupported	
BriefcaseDefinition	Supported	Unsupported	
BriefcaseRule	Supported	Unsupported	
BriefcaseRuleFilter	Supported	Unsupported	
BulkApiResultEvent	Unsupported	Unsupported	
BulkApiResultEventStore	Unsupported	Unsupported	
BusinessBrand	Supported	Supported	
BusinessHours	Supported	Supported	
BusinessProcess	Supported	Supported	
BusinessProcessDefinition	Supported	Unsupported	
BusinessProcessFeedback	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
BusinessProcessGroup	Supported	Unsupported	
BuyerGroupPricebook	Supported	Supported	
Calendar	Supported	Unsupported	
CalendarView	Supported	Supported	
CalendarViewShare	Supported	Supported	
CallCenter	Supported	Unsupported	
CallCoachConfigModifyEvent	Unsupported	Unsupported	
CallCoachingMediaProvider	Supported	Supported	
CallDisposition	Supported	Unsupported	
CallDispositionCategory	Supported	Unsupported	
CallTemplate	Supported	Unsupported	
Campaign	Supported	Supported	
CampaignChangeEvent	Unsupported	Unsupported	
CampaignFeed	Supported	Unsupported	
CampaignHistory	Supported	Unsupported	
CampaignInfluence	Supported	Supported	
CampaignInfluenceModel	Supported	Unsupported	
CampaignMember	Supported	Supported	
CampaignMemberChangeEvent	Unsupported	Unsupported	
CampaignMemberStatus	Supported	Supported	
CampaignMemberStatusChangeEvent	Unsupported	Unsupported	
CampaignOwnerSharingRule	Unsupported	Unsupported	
CampaignShare	Supported	Supported	
CampaignTag	Supported	Unsupported	
CardPaymentMethod	Supported	Supported	
Case	Supported	Supported	
CaseArticle	Supported	Supported	
CaseChangeEvent	Unsupported	Unsupported	
CaseComment	Supported	Supported	
CaseContactRole	Supported	Supported	
CaseExternalDocument	Supported	Supported	
CaseFeed	Supported	Unsupported	
CaseHistory	Unsupported	Unsupported	
CaseMilestone	Supported	Supported	
CaseOwnerSharingRule	Unsupported	Unsupported	
CaseShare	Supported	Supported	
CaseSolution	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
CaseStatus	Supported	Unsupported	
CaseSubjectParticle	Supported	Supported	
CaseTag	Supported	Unsupported	
CaseTeamMember	Supported	Supported	
CaseTeamRole	Supported	Supported	
CaseTeamTemplate	Supported	Supported	
CaseTeamTemplateMember	Supported	Supported	
CaseTeamTemplateRecord	Supported	Unsupported	
CategoryData	Supported	Supported	
CategoryUnsupportedNode	Supported	Supported	
CategoryUnsupportedNodeLocalization	Supported	Supported	
ChannelProgram	Supported	Supported	
ChannelProgramFeed	Supported	Unsupported	
ChannelProgramHistory	Unsupported	Unsupported	
ChannelProgramLevel	Supported	Supported	
ChannelProgramLevelFeed	Supported	Unsupported	
ChannelProgramLevelHistory	Unsupported	Unsupported	
ChannelProgramLevelShare	Supported	Supported	
ChannelProgramMember	Supported	Supported	
ChannelProgramMemberFeed	Supported	Unsupported	
ChannelProgramMemberHistory	Unsupported	Unsupported	
ChannelProgramMemberShare	Supported	Supported	
ChannelProgramShare	Supported	Supported	
ChatterActivity	Supported	Unsupported	
ChatterAnswersActivity	Supported	Unsupported	
ChatterConversation	Supported	Unsupported	
ChatterConversationMember	Supported	Unsupported	
ChatterExtension	Supported	Supported	
ChatterExtensionConfig	Supported	Supported	
ChatterExtensionLocalization	Supported	Supported	
ChatterMessage	Supported	Supported	
ClientBrowser	Supported	Unsupported	
CollaborationGroup	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
CollaborationGroupFeed	Supported	Unsupported	
CollaborationGroupMember	Supported	Supported	
CollaborationGroupMemberRequest	Supported	Supported	
CollaborationGroupRecord	Supported	Supported	
CollaborationInvitation	Supported	Unsupported	
CollabUserEngagementMetric	Supported	Unsupported	
ColorDefinition	Unsupported	Unsupported	
CombinedAttachment	Unsupported	Unsupported	
CommerceEntitlementBuyerGroup	Supported	Unsupported	
CommerceEntitlementPolicy	Supported	Supported	
CommerceEntitlementPolicyShare	Supported	Supported	
CommSubscription	Supported	Supported	
CommSubscriptionChannelType	Supported	Supported	
CommSubscriptionChannelTypeFeed	Supported	Unsupported	
CommSubscriptionChannelTypeHistory	Unsupported	Unsupported	
CommSubscriptionChannelTypeShare	Supported	Supported	
CommSubscriptionConsent	Supported	Supported	
CommSubscriptionConsentChangeEvent	Unsupported	Unsupported	
CommSubscriptionConsentFeed	Supported	Unsupported	
CommSubscriptionConsentHistory	Unsupported	Unsupported	
CommSubscriptionConsentShare	Supported	Supported	
CommSubscriptionFeed	Supported	Unsupported	
CommSubscriptionHistory	Unsupported	Unsupported	
CommSubscriptionShare	Supported	Supported	
CommSubscriptionTiming	Supported	Supported	
CommSubscriptionTimingFeed	Supported	Unsupported	
CommSubscriptionTimingHistory	Unsupported	Unsupported	
Community (Zone)	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
ConferenceNumber	Supported	Supported	
ConnectedApplication	Supported	Unsupported	
ConsumptionRate	Supported	Supported	
ConsumptionRateHistory	Unsupported	Unsupported	
ConsumptionSchedule	Supported	Supported	
ConsumptionScheduleFeed	Supported	Unsupported	
ConsumptionScheduleHistory	Unsupported	Unsupported	
ConsumptionScheduleShare	Supported	Supported	
Contact	Supported	Supported	
ContactChangeEvent	Unsupported	Unsupported	
ContactCleanInfo	Supported	Supported	
ContactFeed	Supported	Unsupported	
ContactHistory	Unsupported	Unsupported	
ContactOwnerSharingRule	Unsupported	Unsupported	
ContactPointAddress	Supported	Supported	
ContactPointAddressChangeEvent	Unsupported	Unsupported	
ContactPointAddressHistory	Unsupported	Unsupported	
ContactPointAddressShare	Supported	Supported	
ContactPointConsent	Supported	Supported	
ContactPointConsentChangeEvent	Unsupported	Unsupported	
ContactPointConsentHistory	Unsupported	Unsupported	
ContactPointConsentShare	Supported	Supported	
ContactPointEmail	Supported	Supported	
ContactPointEmailChangeEvent	Unsupported	Unsupported	
ContactPointEmailHistory	Unsupported	Unsupported	
ContactPointEmailShare	Supported	Supported	
ContactPointPhone	Supported	Supported	
ContactPointPhoneChangeEvent	Unsupported	Unsupported	
ContactPointPhoneHistory	Unsupported	Unsupported	
ContactPointPhoneShare	Supported	Supported	
ContactPointTypeConsent	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
ContactPointTypeConsentChangeEvent	Unsupported	Unsupported	
ContactPointTypeConsentHistory	Unsupported	Unsupported	
ContactPointTypeConsentShare	Supported	Supported	
ContactRequest	Supported	Supported	
ContactRequestShare	Supported	Supported	
ContactShare	Supported	Supported	
ContactTag	Supported	Unsupported	
ContentAsset	Supported	Supported	
ContentBody	Unsupported	Unsupported	
ContentDistribution	Supported	Unsupported	
ContentDistributionView	Supported	Unsupported	
ContentDocument	Supported	Supported	The ContentDocument objects can be restored if the corresponding ContentVersion objects are restored.
ContentDocumentFeed	Supported	Unsupported	
ContentDocumentHistory	Unsupported	Unsupported	
ContentDocumentLink	Supported	Supported	
ContentDocumentListViewMapping	Supported	Supported	
ContentDocumentSubscription	Supported	Unsupported	
ContentFolder	Supported	Supported	
ContentFolderItem	Supported	Unsupported	
ContentFolderLink	Supported	Unsupported	
ContentFolderMember	Unsupported	Unsupported	
ContentHubItem	Unsupported	Unsupported	
ContentHubRepository	Supported	Unsupported	
ContentUnsupportedNote	Supported	Unsupported	
ContentUnsupportedNotification	Supported	Unsupported	
ContentTagSubscription	Supported	Unsupported	
ContentUserSubscription	Supported	Unsupported	
ContentVersion	Supported	Supported	
ContentVersionComment	Supported	Unsupported	
ContentVersionHistory	Unsupported	Unsupported	
ContentVersionRating	Supported	Unsupported	
ContentWorkspace	Supported	Supported	
ContentWorkspaceDoc	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
ContentWorkspaceMember	Supported	Supported	
ContentWorkspacePermission	Supported	Supported	
ContentWorkspaceSubscription	Supported	Unsupported	
Contract	Supported	Supported	
ContractChangeEvent	Unsupported	Unsupported	
ContractContactRole	Supported	Supported	
ContractFeed	Supported	Unsupported	
ContractHistory	Unsupported	Unsupported	
ContractLineItem	Supported	Supported	
ContractLineItemChangeEvent	Unsupported	Unsupported	
ContractLineItemHistory	Unsupported	Unsupported	
ContractStatus	Supported	Unsupported	
ContractTag	Supported	Unsupported	
Conversation	Supported	Unsupported	
ConversationParticipant	Supported	Unsupported	
CorsWhitelistEntry	Supported	Supported	
CronJobDetail	Supported	Unsupported	
CronTrigger	Supported	Unsupported	
CspTrustedSite	Supported	Supported	
CustomBrand	Supported	Supported	
CustomBrandAsset	Supported	Supported	
CustomConsoleComponent	Unsupported	Unsupported	
Customer	Supported	Supported	
CustomHelpMenuItem	Supported	Supported	
CustomHelpMenuSection	Supported	Supported	
CustomHttpHeader	Supported	Unsupported	
CustomUnsupportedNotificationType	Supported	Supported	
CustomObjectUserLicenseMetrics	Supported	Unsupported	
CustomPermission	Supported	Unsupported	
CustomPermissionDependency	Supported	Unsupported	
DandBCompany	Supported	Supported	
Dashboard	Supported	Unsupported	
DashboardComponent	Supported	Unsupported	
DashboardComponentFeed	Supported	Unsupported	
DashboardFeed	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
DashboardTag	Supported	Unsupported	
DataAssessmentFieldMetric	Supported	Unsupported	
DataAssessmentMetric	Supported	Unsupported	
DataAssessmentValueMetric	Supported	Unsupported	
DatacloudAddress	Supported	Unsupported	
DatacloudCompany	Supported	Unsupported	
DatacloudContact	Supported	Unsupported	
DatacloudDandBCompany	Supported	Unsupported	
DatacloudOwnedEntity	Supported	Unsupported	
DataIntegrationRecordPurchasePermission	Supported	Supported	
DatasetExport	Supported	Unsupported	
DatasetExportPart	Supported	Unsupported	
DataStatistics	Supported	Unsupported	
DataType	Supported	Unsupported	
DataUseLegalBasis	Supported	Supported	
DataUseLegalBasisHistory	Unsupported	Unsupported	
DataUseLegalBasisShare	Supported	Supported	
DataUsePurpose	Supported	Supported	
DataUsePurposeHistory	Unsupported	Unsupported	
DataUsePurposeShare	Supported	Supported	
DcSocialProfile	Unsupported	Unsupported	
DcSocialProfileHandle	Unsupported	Unsupported	
DecisionTable	Supported	Unsupported	
DecisionTableDatasetLink	Supported	Unsupported	
DecisionTableParameter	Supported	Unsupported	
DecisionTblDatasetParameter	Supported	Unsupported	
DeclinedEventRelation	Supported	Unsupported	
DelegatedAccount	Supported	Supported	
DelegatedAccountFeed	Supported	Unsupported	
DelegatedAccountHistory	Unsupported	Unsupported	
DelegatedAccountShare	Supported	Supported	
DeleteEvent	Supported	Unsupported	
DigitalSignature	Supported	Supported	
DigitalWallet	Supported	Supported	
Document	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
DocumentAttachmentMap	Supported	Supported	
DocumentChecklistItem	Supported	Unsupported	
DocumentChecklistItemFeed	Supported	Unsupported	
DocumentChecklistItemHistory	Unsupported	Unsupported	
DocumentChecklistItemShare	Supported	Supported	
DocumentTag	Supported	Unsupported	
Domain	Supported	Unsupported	
DomainSite	Supported	Unsupported	
DsarPolicy	Supported	Unsupported	
DsarPolicyLog	Supported	Unsupported	
DuplicateJob	Supported	Supported	
DuplicateJobDefinition	Supported	Unsupported	
DuplicateJobMatchingRule	Supported	Unsupported	
DuplicateJobMatchingRuleDefinition	Supported	Unsupported	
DuplicateRecordItem	Supported	Unsupported	
DuplicateRecordSet	Supported	Supported	
DuplicateRule	Supported	Unsupported	
ElectronicMediaGroup	Supported	Unsupported	
EmailCapture	Supported	Supported	
EmailContent	Supported	Supported	
EmailDomainFilter	Supported	Supported	
EmailDomainKey	Supported	Supported	
EmailMessage	Supported	Supported	
EmailMessageChangeEvent	Unsupported	Unsupported	
EmailMessageRelation	Supported	Supported	
EmailRelay	Supported	Supported	
EmailServicesAddress	Supported	Supported	
EmailServicesFunction	Supported	Supported	
EmailStatus	Unsupported	Unsupported	
EmailTemplate	Supported	Supported	
EmailTemplateChangeEvent	Unsupported	Unsupported	
EmbeddedServiceDetail	Supported	Unsupported	
EmbeddedServiceLabel	Supported	Unsupported	
EngagementChannelType	Supported	Supported	
EngagementChannelTypeFeed	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
EngagementChannelTypeHistory	Unsupported	Unsupported	
EngagementChannelTypeShare	Supported	Supported	
EnhancedLetterhead	Supported	Supported	
EnhancedLetterheadFeed	Supported	Unsupported	
Entitlement	Supported	Supported	
EntitlementChangeEvent	Unsupported	Unsupported	
EntitlementContact	Supported	Unsupported	
EntitlementFeed	Supported	UnsupportedUnsupported	
EntitlementHistory			
EntitlementTemplate	Supported	Supported	
EntityDefinition	Supported	Unsupported	
EntityHistory	Unsupported	Unsupported	
EntityMilestone	Supported	Supported	
EntityMilestoneFeed	Supported	Unsupported	
EntityMilestoneHistory	Unsupported	Unsupported	
EntityParticle	Supported	Unsupported	
EntitySubscription	Supported	Unsupported	
Event	Supported	Supported	
EventBusSubscriber	Supported	Unsupported	
EventChangeEvent	Unsupported	Unsupported	
EventFeed	Supported	Unsupported	
EventLogFile	Supported	Unsupported	
EventRelation	Supported	Supported	
EventRelationChangeEvent	Unsupported	Unsupported	
EventTag	Supported	Unsupported	
EventWhoRelation	Supported	Unsupported	
Expense	Supported	Supported	
ExpenseReport	Supported	Supported	
ExpenseReportEntry	Supported	Supported	
ExpressionFilter	Supported	Supported	
ExpressionFilterCriteria	Supported	Supported	
ExternalAccountHierarchyHistory	Unsupported	Unsupported	
ExternalDataSource	Supported	Unsupported	
ExternalDataUserAuth	Supported	Supported	
ExternalEvent	Supported	Supported	
ExternalEventMapping	Supported	Supported	
ExternalEventMappingShare	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
ExternalSocialAccount	Supported	Unsupported	
FAQ__DataCategorySelection	Supported	Supported	
FAQ__Feed	Supported	Unsupported	
FAQ__ka	Supported	Unsupported	
FAQ__kav	Supported	Supported	
FAQ__VersionHistory	Unsupported	Unsupported	
FAQ__ViewStat	Supported	Unsupported	
FAQ__VoteStat	Supported	Unsupported	
FeedAttachment	Supported	Supported	
FeedComment	Supported	Supported	
FeedItem	Supported	Supported	
FeedLike	Unsupported	Unsupported	
FeedPollChoice	Supported	Unsupported	
FeedPollVote	Supported	Unsupported	
FeedRevision	Supported	Unsupported	
feedSignal	Unsupported	Unsupported	
FeedTrackedChange	Unsupported	Unsupported	
FieldDefinition	Supported	Unsupported	
FieldHistoryArchive	Unsupported	Unsupported	
FieldPermissions	Supported	Supported	
FieldSecurityActivity	Supported	Unsupported	
FieldSecurityClassification	Supported	Unsupported	
FieldServiceMobileSettings	Supported	Supported	
FileEvent	Unsupported	Unsupported	
FileEventStore	Unsupported	Unsupported	
FileSearchActivity	Supported	Unsupported	
FiscalYearSettings	Supported	Unsupported	
FlexQueueItem	Supported	Unsupported	
FlowDefinitionView	Supported	Unsupported	
FlowExecutionErrorEvent	Unsupported	Unsupported	
FlowInterview	Supported	Unsupported	
FlowInterviewLog	Supported	Unsupported	
FlowInterviewLogEntry	Supported	Unsupported	
FlowInterviewLogShare	Supported	Supported	
FlowInterviewOwnerSharingRule	Unsupported	Unsupported	
FlowInterviewShare	Supported	Supported	
FlowOrchestrationInstance	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
FlowOrchestrationStageInstance	Supported	Supported	
FlowOrchestrationStepInstance	Supported	Supported	
FlowOrchestrationWorkItem	Supported	Supported	
FlowRecordRelation	Supported	Supported	
FlowStageRelation	Supported	Unsupported	
FlowVariableView	Unsupported	Unsupported	
FlowVersionView	Unsupported	Unsupported	
Folder	Supported	Supported	
FolderedContentDocument	Unsupported	Unsupported	
ForecastingDisplayedFamily	Supported	Unsupported	
ForecastingFact	Supported	Unsupported	
ForecastingItem	Supported	Unsupported	
ForecastingType	Supported	Supported	
ForecastingTypeSource	Supported	Supported	
FormulaFunction	Supported	Unsupported	
FormulaFunctionAllowedType	Supported	Unsupported	
FormulaFunctionCategory	Supported	Unsupported	
GoalHistory	Unsupported	Unsupported	
GrantedByLicense	Supported	Unsupported	
Group	Supported	Supported	
GroupMember	Supported	Unsupported	
GuestBuyerProfile	Supported	Unsupported	
HashtagDefinition	Supported	Unsupported	
Holiday	Supported	Supported	
IconDefinition	Supported	Unsupported	
Idea	Supported	Supported	
IdeaComment	Supported	Supported	
IdeaReputation	Supported	Unsupported	
IdeaReputationLevel	Supported	Supported	
IdeaTheme	Supported	Supported	
IdentityProviderEventStore	Unsupported	Unsupported	
IdentityVerificationEvent	Unsupported	Unsupported	
IdpEventLog	Supported	Unsupported	
IframeWhiteListUrl	Supported	Supported	
Image	Supported	Supported	
ImageShare	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
Individual	Supported	Supported	
IndividualChangeEvent	Unsupported	Unsupported	
IndividualHistory	Unsupported	Unsupported	
IndividualShare	Supported	Supported	
InstalledMobileApp	Supported	Unsupported	
Instruction__DataCategorySelection	Supported	Supported	
Instruction__ka	Supported	Unsupported	
Instruction__kav	Supported	Supported	
Instruction__ViewStat	Supported	Unsupported	
Instruction__VoteStat	Supported	Unsupported	
JobProfile	Supported	Supported	
Knowledge__DataCategorySelection	Supported	Unsupported	
Knowledge__Feed	Supported	Unsupported	
Knowledge__ka	Supported	Unsupported	
Knowledge__kav	Supported	Supported	
Knowledge__Share	Supported	Supported	
Knowledge__ViewStat	Supported	Unsupported	
Knowledge__VoteStat	Supported	Unsupported	
KnowledgeableUser	Supported	Unsupported	
KnowledgeArticle	Supported	Unsupported	
KnowledgeArticleVersion	Supported	Unsupported	
KnowledgeArticleVersionHistory	Unsupported	Unsupported	
KnowledgeArticleViewStat	Supported	Unsupported	
KnowledgeArticleVoteStat	Supported	Unsupported	
Lead	Supported	Supported	
LeadChangeEvent	Unsupported	Unsupported	
LeadCleanInfo	Supported	Supported	
LeadFeed	Unsupported	Unsupported	
LeadHistory	Unsupported	Unsupported	
LeadShare	Supported	Supported	
LeadStatus	Supported	Unsupported	
LeadTag	Supported	Unsupported	
LegalEntity	Supported	Supported	
LightningExitByPageMetrics	Supported	Unsupported	
LightningExperienceTheme	Supported	Supported	
LightningOnboardingConfig	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
LightningToggleMetrics	Supported	Unsupported	
LightningUriEvent	Unsupported	Unsupported	
LightningUriEventStream	Unsupported	Unsupported	
LightningUsageByAppTypeMetrics	Supported	Unsupported	
LightningUsageByBrowserMetrics	Supported	Unsupported	
LightningUsageByFlexiPageMetrics	Supported	Unsupported	
LightningUsageByPageMetrics	Supported	Unsupported	
LinkedArticle	Supported	Supported	
LinkedArticleFeed	Supported	Unsupported	
LinkedArticleHistory		Unsupported	
ListEmail	Supported	Supported	
ListEmailChangeEvent	Unsupported	Unsupported	
ListEmailIndividualRecipient	Supported	Supported	
ListEmailRecipientSource	Supported	Supported	
ListEmailShare	Supported	Supported	
ListView	Supported	Unsupported	
ListViewChart	Supported	Supported	
ListViewChartInstance	Supported	Unsupported	
ListViewEvent	Unsupported	Unsupported	
ListViewEventStream	Unsupported	Unsupported	
LiveAgentSession	Supported	Unsupported	
LiveAgentSessionHistory	Unsupported	Unsupported	
LiveAgentSessionShare	Supported	Supported	
LiveChatBlockingRule	Supported	Supported	
LiveChatButton	Supported	Supported	
LiveChatButtonDeployment	Supported	Supported	
LiveChatButtonSkill	Supported	Unsupported	
LiveChatDeployment	Supported	Supported	
LiveChatSensitiveDataRule	Supported	Supported	
LiveChatTranscript	Supported	Supported	
LiveChatTranscriptEvent	Supported	Supported	
LiveChatTranscriptShare	Supported	Supported	
LiveChatUserConfig	Supported	Supported	
LiveChatUserConfigUser	Supported	Supported	
Location	Supported	Supported	
LocationChangeEvent	Unsupported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
LocationFeed	Supported	Unsupported	
LocationGroup	Supported	Supported	
LocationHistory	Unsupported	Unsupported	
LocationShare	Supported	Supported	
LocationTrustMeasure	Supported	Supported	
LocationTrustMeasureShare	Supported	Supported	
LoginAsEvent	Unsupported	Unsupported	
LoginAsEventStream	Unsupported	Unsupported	
LoginEvent	Unsupported	Unsupported	
LoginEventStream	Unsupported	Unsupported	
LoginGeo	Supported	Unsupported	
LoginHistory	Unsupported	Unsupported	
LoginIp	Supported	Unsupported	
LogoutEvent	Unsupported	Unsupported	
LogoutEventStream	Unsupported	Unsupported	
LookedUpFromActivity	Unsupported	Unsupported	
Macro	Supported	Supported	
MacroChangeEvent	Unsupported	Unsupported	
MacroHistory	Unsupported	Unsupported	
MacroInstructionChangeEvent		Unsupported	
MacroShare	Supported	Supported	
MacroUsage	Supported	Unsupported	
MacroUsageShare	Supported	Supported	
MailmergeTemplate	Supported	Supported	
MaintenanceAsset	Supported	Supported	
MaintenancePlan	Supported	Supported	
MaintenanceWorkRule	Supported	Supported	
ManagedContentInfo	Unsupported	Unsupported	
MatchingInformation	Supported	Unsupported	
MatchingRule	Supported	Unsupported	
MatchingRuleItem	Supported	Unsupported	
MetadataPackage	Supported	Unsupported	
MetadataPackageVersion	Supported	Unsupported	
Metric	Unsupported	Unsupported	
MetricDataLink	Unsupported	Unsupported	
MetricDataLinkHistory	Unsupported	Unsupported	
MetricHistory	Unsupported	Unsupported	
MetricsDataFile	Unsupported	Unsupported	
MilestoneType	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
MLField	Supported	Unsupported	
MlIntentUtteranceSuggestion	Supported	Unsupported	
MLPredictionDefinition	Supported	Unsupported	
MLRecommendationDefinition	Unsupported	Unsupported	
MobileApplicationDetail	Supported	Supported	
MobileSecurityUserMetric	Unsupported	Unsupported	
MobileSettingsAssignment	Supported	Supported	
MsgChannelLanguageKeyword	Supported	Unsupported	
MutingPermissionSet	Supported	Supported	
MyDomainDiscoverableLogin	Supported	Supported	
Name	Unsupported	Unsupported	
NamedCredential	Supported	Unsupported	
NamedspaceRegistryFeed	Supported	Unsupported	
NamespaceRegistryHistory	UnsupportedUnsupported		
NavigationMenuItem	Supported	Supported	
NavigationMenuItemLocalization	Supported	Supported	
Network	Supported	Unsupported	
NetworkActivityAudit	Supported	Supported	
NetworkAffinity	Supported	Supported	
NetworkDiscoverableLogin	Supported	Supported	
NetworkFeedResponseMetric	Supported	Unsupported	
NetworkMember	Supported	Unsupported	
NetworkMemberGroup	Supported	Supported	
NetworkModeration	Supported	Supported	
NetworkPageOverride	Supported	Supported	
NetworkSelfRegistration	Supported	Supported	
NetworkUserHistoryRecent	Supported	Supported	
Note	Supported	Supported	
NoteAndAttachment	Unsupported	Unsupported	
OauthCustomScope	Supported	Supported	
OauthCustomScopeApp	Supported	Supported	
OauthToken	Supported	Unsupported	
ObjectPermissions	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
ObjectTerritory2AssignmentRule	Supported	Supported	
ObjectTerritory2AssignmentRuleItem	Supported	Supported	
ObjectTerritory2Association	Supported	Supported	
OmniDataTransform	Supported	Supported	
OmniDataTransformItem	Supported	Supported	
OmniInteractionConfig	Supported	Supported	
OmniProcess	Supported	Supported	
OmniProcessCompilation	Supported	Supported	
OmniProcessElement	Supported	Supported	
OmniScriptSavedSession	Supported	Supported	
OmniSupervisorConfig	Supported	Supported	
OmniSupervisorConfigGroup	Supported	Supported	
OmniSupervisorConfigProfile	Supported	Supported	
OmniSupervisorConfigUser	Supported	Supported	
OmniUiCard	Supported	Supported	
OpenActivity	Unsupported	Unsupported	
OperatingHours	Supported	Supported	
OperatingHoursHistory	Unsupported	Unsupported	
OperatingHoursHoliday	Supported	Supported	
Opportunity	Supported	Supported	
OpportunityChangeEvent	Unsupported	Unsupported	
OpportunityCompetitor	Supported	Supported	
OpportunityContactRole	Supported	Supported	
OpportunityContactRoleChangeEvent	Unsupported	Unsupported	
OpportunityContactRoleSuggestionInsight	Supported	Unsupported	
OpportunityFeed	Supported	Unsupported	
OpportunityFieldHistory	Unsupported	Unsupported	
OpportunityHistory	Unsupported	Unsupported	
OpportunityLineItem	Supported	Supported	
OpportunityLineItemSchedule	Supported	Supported	
OpportunityOwnerSharingRule	Unsupported	Unsupported	
OpportunityPartner	Supported	Unsupported	
OpportunityShare	Supported	Supported	
OpportunitySplit	Supported	Supported	
OpportunitySplitType	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
OpportunityStage	Supported	Unsupported	
OpportunityTag	Supported	Unsupported	
OpportunityTeamMember	Supported	Supported	
Order	Supported	Supported	
OrderAdjustmentGroup	Supported	Supported	
OrderChangeEvent	Unsupported	Unsupported	
OrderDeliveryGroup	Supported	Supported	
OrderDeliveryMethod	Supported	Supported	
OrderFeed	Supported	Unsupported	
OrderHistory	Unsupported	Unsupported	
OrderItem	Supported	Supported	
OrderItemAdjustmentLineItem	Supported	Supported	
OrderItemChangeEvent	Unsupported	Unsupported	
OrderItemFeed	Supported	Unsupported	
OrderItemHistory	Unsupported	Unsupported	
OrderItemTaxLineItem	Supported	Supported	
OrderItemType	Supported	Unsupported	
OrderOwnerSharingRule	Unsupported	Unsupported	
OrderShare	Supported	Unsupported	
OrderStatus	Supported	Unsupported	
OrderTag	Supported	Unsupported	
Organization	Supported	Supported	
OrgDeleteRequest	Supported	Unsupported	
OrgLifecycleNotification	Unsupported	Unsupported	
OrgMetric	Supported	Supported	
OrgMetricScanResult	Supported	Supported	
OrgMetricScanSummary	Supported	Supported	
OrgWideEmailAddress	Supported	Supported	
OutgoingEmail	Unsupported	Unsupported	
OutgoingEmailRelation	Unsupported	Unsupported	
OutOfOffice	Supported	Supported	
OwnedContentDocument	Unsupported	Unsupported	
OwnerChangeOptionInfo	Unsupported	Unsupported	
PackageLicense	Supported	Unsupported	
PackagePushError	Supported	Unsupported	
PackagePushJob	Supported	Supported	
PackagePushRequest	Supported	Supported	
PackageSubscriber	Supported	Unsupported	
Partner	Supported	Unsupported	
PartnerFundAllocation	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
PartnerFundAllocationFeed	Supported	Unsupported	
PartnerFundAllocationHistory	Unsupported	Unsupported	
PartnerFundAllocationShare	Supported	Supported	
PartnerFundClaim	Supported	Supported	
PartnerFundClaimFeed	Supported	Unsupported	
PartnerFundClaimHistory	Unsupported	Unsupported	
PartnerFundClaimShare	Supported	Supported	
PartnerFundRequest	Supported	Supported	
PartnerFundRequestFeed	Supported	Unsupported	
PartnerFundRequestHistory	Unsupported	Unsupported	
PartnerFundRequestShare	Supported	Supported	
PartnerMarketingBudget	Supported	Supported	
PartnerMarketingBudgetFeed	Supported	Unsupported	
PartnerMarketingBudgetHistory	Unsupported	Unsupported	
PartnerMarketingBudgetShare	Supported	Supported	
PartnerUnsupportedetworkConnection	Supported	Unsupported	
PartnerUnsupportedetworkRecordConnection	Supported	Unsupported	
PartnerUnsupportedetworkSyncLog	Supported	Unsupported	
PartnerRole	Supported	Unsupported	
PartyConsent	Supported	Supported	
PartyConsentChangeEvent	Unsupported	Unsupported	
PartyConsentFeed	Supported	Unsupported	
PartyConsentHistory	Unsupported	Unsupported	
PartyConsentShare	Supported	Supported	
Payment	Supported	Supported	
PaymentAuthAdjustment	Supported	Supported	
PaymentAuthorization	Supported	Supported	
PaymentGateway	Supported	Supported	
PaymentGatewayLog	Supported	Supported	
PaymentGatewayProvider	Supported	Supported	
PaymentGroup	Supported	Supported	
PaymentMethod	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
PendingServiceRouting	Supported	Supported	
PendingServiceRoutingShare	Supported	Supported	
Period	Supported	Unsupported	
PermissionSet	Supported	Supported	
PermissionSetAssignment	Supported	Supported	
PermissionSetEvent	Unsupported	Unsupported	
PermissionSetEventStore	Unsupported	Unsupported	
PermissionSetGroup	Supported	Supported	
PermissionSetGroupComponent	Supported	Supported	
PermissionSetLicense	Supported	Unsupported	
PermissionSetLicenseAssign	Supported	Supported	
PermissionSetTabSetting	Supported	Supported	
PersonalizationTargetInfo	Supported	Unsupported	
PicklistValueInfo	Supported	Unsupported	
PlatformAction	Unsupported	Unsupported	
PlatformCachePartition	Supported	Supported	
PlatformCachePartitionType	Supported	Supported	
PlatformEventUsageMetric	Supported	Unsupported	
PlatformStatusAlertEvent	Unsupported	Unsupported	
PortalDelegablePermissionSet	Supported	Supported	
PresenceConfigDeclineReason	Supported	Supported	
PresenceUserConfig	Supported	Supported	
PresenceUserConfigProfile	Supported	Supported	
PriceAdjustmentSchedule	Supported	Supported	
PriceAdjustmentTier	Supported	Supported	
Pricebook2	Supported	Supported	
Pricebook2ChangeEvent	Supported	Supported	
Pricebook2History	Supported	Supported	
PricebookEntry	Supported	Supported	
PricebookEntryAdjustment	Supported	Supported	
PricebookEntryHistory	Supported	Unsupported	
ProcessDefinition	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
ProcessException	Supported	Supported	
ProcessInstance	Supported	Unsupported	
ProcessInstanceHistory	Unsupported	Unsupported	
ProcessInstanceNode	Supported	Unsupported	
ProcessInstanceStep	Supported	Unsupported	
ProcessInstanceWorkitem	Supported	Supported	
ProcessNode	Supported	Unsupported	
Product2	Supported	Supported	
Product2ChangeEvent	Unsupported	Unsupported	
Product2DataTranslation	Supported	Supported	
Product2Feed	Supported	Unsupported	
Product2History	Unsupported	Unsupported	
ProductAttribute	Supported	Supported	
ProductCatalog	Supported	Supported	
ProductCategory	Supported	Supported	
ProductCategoryDataTranslation	Supported	Supported	
ProductCategoryProduct	Supported	Supported	
ProductConsumed	Supported	Supported	
ProductConsumptionSchedule	Supported	Supported	
ProductEntitlementTemplate	Supported	Supported	
ProductFulfillmentLocation	Supported	Supported	
ProductFulfillmentLocationFeed	Supported	Unsupported	
ProductFulfillmentLocationHistory	Unsupported	Unsupported	
ProductFulfillmentLocationShare	Supported	Supported	
ProductItemChangeEvent	Unsupported	Unsupported	
ProductItemFeed	Supported	Unsupported	
ProductItemHistory	Unsupported	Unsupported	
ProductItemShare	Supported	Supported	
ProductItem	Supported	Supported	
ProductItemTransaction	Supported	Supported	
ProductItemTransactionFeed	Supported	Unsupported	
ProductItemTransactionHistory	Unsupported	Unsupported	
ProductMedia	Supported	Supported	
ProductRelationshipType	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
ProductRequest	Supported	Supported	
ProductRequestLineItem	Supported	Supported	
ProductRequired	Supported	Supported	
ProductRequiredFeed	Supported	Unsupported	
ProductRequiredHistory	Unsupported	Unsupported	
ProductServiceCampaign	Supported	Unsupported	
ProductServiceCampaignItemStatus	Supported	Unsupported	
ProductServiceCampaignStatus	Supported	Unsupported	
ProductTransfer	Supported	Supported	
ProductTransferChangeEvent	Unsupported	Unsupported	
ProductTransferFeed	Supported	Unsupported	
ProductTransferHistory	Unsupported	Unsupported	
ProductTransferShare	Supported	Supported	
Profile	Supported	Unsupported	
ProfileSkill	Supported	Supported	
ProfileSkillEndorsement	Supported	Supported	
ProfileSkillEndorsementFeed	Supported	Unsupported	
ProfileSkillEndorsementHistory	Unsupported	Unsupported	
ProfileSkillFeed	Supported	Unsupported	
ProfileSkillHistory	Unsupported	Unsupported	
ProfileSkillShare	Supported	Supported	
ProfileSkillUser	Supported	Supported	
ProfileSkillUserFeed	Supported	Unsupported	
ProfileSkillUserHistory	Unsupported	Unsupported	
Prompt	Supported	Supported	
PromptAction	Supported	Supported	
PromptActionOwnerSharingRule	Unsupported	Unsupported	
PromptActionShare	Supported	Supported	
PromptError	Supported	Supported	
PromptLocalization	Supported	Supported	
PromptVersion	Supported	Supported	
PromptVersionLocalization	Supported	Supported	
Publisher	Supported	Unsupported	
PushTopic	Supported	Supported	
QuestionDataCategorySelection	Supported	Unsupported	
QuestionReportAbuse	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
QueueRoutingConfig	Supported	Supported	
QueueSobject	Supported	Supported	
QuickText	Supported	Supported	
QuickTextChangeEvent	Unsupported	Unsupported	
QuickTextHistory	Unsupported	Unsupported	
QuickTextShare	Supported	Supported	
QuickTextUsage	Supported	Unsupported	
QuickTextUsageShare	Supported	Supported	
Quote	Supported	Supported	
QuoteChangeEvent	Unsupported	Unsupported	
QuoteDocument	Supported	Unsupported	
QuoteFeed	Supported	Unsupported	
QuoteLineItem	Supported	Supported	
QuoteLineItemChangeEvent	Unsupported	Unsupported	
QuoteShare	Supported	Supported	
QuoteTemplateRichTextData	Supported	Unsupported	
RecentFieldChange	Supported	Unsupported	
RecentlyViewed	Supported	Unsupported	
Recommendation	Supported	Supported	
RecommendationChangeEvent	Unsupported	Unsupported	
RecordAction	Supported	Supported	
RecordActionHistory	Unsupported	Unsupported	
RecordsetFilterCriteria	Supported	Supported	
RecordsetFilterCriteriaRule	Supported	Supported	
RecordType	Supported	Supported	
RecordTypeLocalization	Supported	Supported	
RecordVisibility (Pilot)	Supported	Unsupported	
RedirectWhitelistUrl	Supported	Supported	
Refund	Supported	Supported	
RefundLinePayment	Supported	Supported	
RelationshipDomain	Supported	Unsupported	
RelationshipInfo	Supported	Unsupported	
ReplyReportAbuse	Supported	Unsupported	
Report	Supported	Unsupported	
ReportEvent	Unsupported	Unsupported	
ReportEventStream	Unsupported	Unsupported	
ReportFeed	Supported	Unsupported	
ReportTag	Supported	Unsupported	
ReputationLevel	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
ReputationLevelLocalization	Supported	Supported	
ReputationPointsRule	Supported	Unsupported	
ResourceAbsence	Supported	Supported	
ResourcePreference	Supported	Supported	
ReturnOrder	Supported	Supported	
ReturnOrderOwnerSharingRule	Unsupported	Unsupported	
RuleTerritory2Association	Supported	Supported	
SalesAIScoreCycle	Supported	Unsupported	
SalesAIScoreModelFactor	Supported	Unsupported	
SalesStoreCatalog	Supported	Unsupported	
SamlSsoConfig	Supported	Unsupported	
SchedulingConstraint	Supported	Supported	
Scontrol	Supported	Supported	
ScontrolLocalization	Supported	Supported	
Scorecard	Supported	Supported	
ScorecardAssociation	Supported	Supported	
ScorecardMetric	Supported	Supported	
ScratchOrgInfo	Supported	Supported	
ScratchOrgInfoFeed	Supported	Unsupported	
ScratchOrgInfoHistory	Unsupported	Unsupported	
SearchActivity	Supported	Unsupported	
SearchLayout	Supported	Unsupported	
SearchPromotionRule	Supported	Supported	
SecureAgent	Supported	Unsupported	
SecureAgentPlugin	Unsupported	Unsupported	
SecureAgentPluginProperty	Unsupported	Unsupported	
SecureAgentsCluster	Supported	Unsupported	
SecurityCustomBaseline	Supported	Supported	
Seller	Supported	Unsupported	
ServiceAppointment	Supported	Supported	
ServiceAppointmentStatus	Supported	Unsupported	
ServiceChannel	Supported	Supported	
ServiceChannelStatus	Supported	Supported	
ServiceContract	Supported	Supported	
ServiceContractChangeEvent	Unsupported	Unsupported	
ServiceContractFeed	Supported	Unsupported	
ServiceContractHistory	Unsupported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
ServiceContractShare	Supported	Supported	
ServiceCrew	Supported	Supported	
ServiceCrewMember	Supported	Supported	
ServiceCrewOwnerSharingRule	Unsupported	Unsupported	
ServiceFieldDataType	Unsupported	Unsupported	
ServicePresenceStatus	Supported	Supported	
ServiceReport	Supported	Supported	
ServiceReportLayout	Supported	Unsupported	
ServiceResource	Supported	Unsupported	
ServiceResourceCapacity	Supported	Supported	
ServiceResourceCapacity History	Unsupported	Unsupported	
ServiceResourceChange Event	Unsupported	Unsupported	
ServiceResourceFeed	Supported	Unsupported	
ServiceResourceHistory	Unsupported	Unsupported	
ServiceResourceOwnerSharingRule	Unsupported	Unsupported	
ServiceResourcePreference	Supported	Supported	
ServiceResourceShare	Supported	Supported	
ServiceResourceSkill	Supported	Supported	
ServiceTerritory	Supported	Supported	
ServiceTerritoryLocation	Supported	Supported	
ServiceTerritoryMember	Supported	Supported	
SessionPermSetActivation	Supported	Unsupported	
SetupAuditTrail	Supported	Unsupported	
SetupEntityAccess	Supported	Unsupported	
ShapeRepresentation	Supported	Supported	
Shift	Supported	Supported	
ShiftHistory	Unsupported	Unsupported	
ShiftOwnerSharingRule	Unsupported	Unsupported	
ShiftShare	Supported	Supported	
Shipment	Supported	Supported	
ShipmentChangeEvent	Unsupported	Unsupported	
ShipmentFeed	Supported	Unsupported	
ShipmentHistory	Unsupported	Unsupported	
ShipmentShare	Supported	Supported	
ShipmentItem	Supported	Supported	
Site	Supported	Unsupported	
SiteDetail	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
SiteDomain	Supported	Unsupported	
SiteFeed	Supported	Unsupported	
SiteHistory	Unsupported	Unsupported	
SiteIframeWhitelistUrl	Supported	Supported	
Skill	Supported	Supported	
SkillProfile	Supported	Supported	
SkillRequirement	Supported	Supported	
SkillUser	Supported	Supported	
SlaProcess	Supported	Unsupported	
SocialPersona	Supported	Supported	
SocialPersonaHistory	Unsupported	Unsupported	
SocialPost	Supported	Supported	
SocialPostChangeEvent	Unsupported	Unsupported	
SocialPostFeed	Supported	Unsupported	
SocialPostHistory	Unsupported	Unsupported	
SocialPostShare	Supported	Supported	
Solution	Supported	Supported	
SolutionFeed	Supported	Unsupported	
SolutionHistory	Unsupported	Unsupported	
SolutionStatus	Supported	Unsupported	
SolutionTag	Supported	Unsupported	
SOSDeployment	Supported	Supported	
SOSSession	Supported	Supported	
SOSSessionActivity	Supported	Supported	
SOSSessionFeed	Supported	Unsupported	
SOSSessionHistory	Unsupported	Unsupported	
SOSSessionShare	Supported	Supported	
SPSamlAttributes	Supported	Supported	
Stamp	Supported	Supported	
StampAssignment	Supported	Supported	
StampLocalization	Supported	Supported	
Standardobject__hd	Supported	Unsupported	
StaticResource	Supported	Supported	
StreamingChannel	Supported	Supported	
StreamingChannelShare	Supported	Supported	
Survey	Supported	Unsupported	
SurveyEmailBranding	Supported	Supported	
SurveyEngagementContext	Supported	Supported	
SurveyEngagementContextShare	Supported	Supported	
SurveyFeed	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
SurveyInvitation	Supported	Supported	
SurveyInvitationShare	Supported	Supported	
SurveyPage	Supported	Unsupported	
SurveyQuestion	Supported	Unsupported	
SurveyQuestionChoice	Supported	Unsupported	
SurveyQuestionResponse	Supported	Unsupported	
SurveyQuestionScore	Supported	Unsupported	
SurveyResponse	Supported	Unsupported	
SurveyShare	Supported	Supported	
SurveySubject	Supported	Supported	
SurveyVersion	Supported	Unsupported	
SurveyVersionAddlInfo	Supported	Unsupported	
TabDefinition	Supported	Unsupported	
TagDefinition	Supported	Supported	
Task	Supported	Supported	
TaskChangeEvent	Unsupported	Unsupported	
TaskFeed	Supported	Unsupported	
TaskPriority	Supported	Unsupported	
TaskRelation	Supported	Supported	
TaskRelationChangeEvent	Unsupported	Unsupported	
TaskStatus	Supported	Unsupported	
TaskTag	Supported	Unsupported	
TaskWhoRelation	Supported	Unsupported	
TenantSecret	Supported	Supported	
TenantSecurityMonitorMetric	Supported	Unsupported	Due to a current issue with the Salesforce API, queries are returning errors. As a result, our backup job may also fail.
TenantUsageEntitlement	Supported	Unsupported	
Territory2	Supported	Supported	
Territory2Model	Supported	Supported	
Territory2ModelFeed	Supported	Unsupported	
Territory2ModelHistory	Unsupported	Unsupported	
Territory2Type	Supported	Supported	
TestSuiteMembership	Supported	Supported	
ThirdPartyAccountLink	Supported	Unsupported	
TimeSheet	Supported	Supported	
TimeSheetEntry	Supported	Supported	
TimeSlot	Supported	Supported	
TimeSlotHistory	Unsupported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
TodayGoal	Supported	Supported	
TodayGoalShare	Supported	Supported	
Topic	Supported	Supported	
TopicAssignment	Supported	Unsupported	
TopicFeed	Supported	Unsupported	
TopicLocalization	Supported	Supported	
TopicUserEvent	Supported	Unsupported	
Translation	Supported	Supported	
UiFormulaCriterion	Supported	Unsupported	
UiFormulaRule	Supported	Unsupported	
UndecidedEventRelation	Supported	Unsupported	
UnifiedActivity	Unsupported	Unsupported	
UnifiedActivityParticipant	Unsupported	Unsupported	
UnifiedActivityRelation	Unsupported	Unsupported	
UnifiedEmail	Unsupported	Unsupported	
UnifiedEmailParticipant	Unsupported	Unsupported	
UnifiedMeeting	Unsupported	Unsupported	
UnifiedMeetingParticipant	Unsupported	Unsupported	
UnifiedTask	Unsupported	Unsupported	
UnifiedTaskParticipant	Unsupported	Unsupported	
UnifiedVideoCall	Unsupported	Unsupported	
UnifiedVideoCallParticipant	Unsupported	Unsupported	
UnifiedVoiceCall	Unsupported	Unsupported	
UnifiedVoiceCallParticipant	Unsupported	Unsupported	
UriEvent	Unsupported	Unsupported	
UriEventStream	Unsupported	Unsupported	
User	Supported	Supported	
UserAccountTeamMember	Supported	Supported	
UserAppInfo	Supported	Supported	
UserAppMenuCustomization	Supported	Supported	
UserAppMenuCustomizationShare	Supported	Supported	
UserAppMenuItem	Supported	Unsupported	
UserChangeEvent	Unsupported	Unsupported	
UserConfigTransferButton	Supported	Supported	
UserConfigTransferSkill	Supported	Supported	
UserCustomBadge	Supported	Supported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
UserCustomBadgeLocalization	Supported	Supported	
UserDeviceHistory	Unsupported	Unsupported	
UserEmailPreferredPerson	Supported	Supported	
UserEmailPreferredPersonShare	Supported	Supported	
UserEntityAccess	Supported	Unsupported	
UserFeed	Supported	Unsupported	
UserFieldAccess	Supported	Unsupported	
UserLicense	Supported	Unsupported	
UserListView	Supported	Supported	
UserListViewCriterion	Supported	Supported	
UserLogin	Supported	Supported	
UserPackageLicense	Supported	Supported	
UserPermissionAccess	Supported	Unsupported	
UserPreference	Supported	Supported	
UserProvAccount	Supported	Supported	
UserProvAccountStaging	Supported	Supported	
UserProvisioningConfig	Supported	Supported	
UserProvisioningLog	Supported	Supported	
UserProvisioningRequest	Supported	Supported	
UserProvisioningRequestShare	Supported	Supported	
UserProvMockTarget	Supported	Supported	
UserRecordAccess	Supported	Unsupported	
UserRole	Supported	Supported	
UserServicePresence	Supported	Supported	
UserSetupEntityAccess	Supported	Unsupported	
UserShare	Supported	Supported	
UserTeamMember	Supported	Supported	
UserTerritory2Association	Supported	Supported	
VerificationHistory	Unsupported	Unsupported	
VideoCallParticipant	Supported	Unsupported	
VideoCallRecording	Supported	Unsupported	
Visit	Supported	Supported	
VisitedParty	Supported	Supported	
VisitedPartyFeed	Supported	Unsupported	
VisitedPartyHistory	Unsupported	Unsupported	
VisitFeed	Supported	Unsupported	
Visitor	Supported	Supported	
VisitorFeed	Supported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
VisitorHistory	Unsupported	Unsupported	
VisitShare	Supported	Supported	
VisualforceAccessMetrics	Supported	Unsupported	
VoiceCallQualityFeedback	Supported	Unsupported	
VoiceCoaching	Supported	Unsupported	
VoiceLocalPresenceNumber	Supported	Unsupported	
VoiceVendorInfo	Supported	Unsupported	
VoiceVendorLine	Supported	Unsupported	
Vote	Supported	Supported	
WarrantyTerm	Supported	Supported	
WaveAutoInstallRequest	Supported	Supported	
WaveCompatibilityCheckItem	Supported	Unsupported	
WebCartHistory	Unsupported	Unsupported	
WebLink	Supported	Supported	
WebLinkLocalization	Supported	Supported	
WebStore	Supported	Supported	
WebStoreCatalog	Supported	Supported	
WebStorePricebook	Supported	Supported	
Wishlist	Supported	Supported	
WishlistItem	Supported	Supported	
WorkAccess	Supported	Supported	
WorkAccessShare	Supported	Supported	
WorkBadge	Supported	Supported	
WorkBadgeDefinition	Supported	Supported	
WorkBadgeDefinitionFeed	Supported	Unsupported	
WorkBadgeDefinitionHistory	Unsupported	Unsupported	
WorkBadgeDefinitionShare	Supported	Supported	
WorkCoachingHistory	Unsupported	Unsupported	
WorkFeedbackHistory	Unsupported	Unsupported	
WorkFeedbackQuestionHistory	Unsupported	Unsupported	
WorkFeedbackQuestionSetHistory	Supported	Unsupported	
WorkGoalCollaboratorHistory	Unsupported	Unsupported	
WorkGoalHistory	Unsupported	Unsupported	
WorkOrder	Supported	Supported	
WorkOrderChangeEvent	Unsupported	Unsupported	

Object Name	Support Status in Backup	Support Status in Restore	Comments
WorkOrderFeed	Supported	Unsupported	
WorkOrderHistory	Unsupported	Unsupported	
WorkOrderLineItem	Supported	Supported	
WorkOrderLineItemChangeEvent	Unsupported	Unsupported	
WorkOrderLineItemFeed	Supported	Unsupported	
WorkOrderLineItemHistory	Unsupported	Unsupported	
WorkOrderLineItemStatus	Supported	Unsupported	
WorkOrderShare	Supported	Supported	
WorkOrderStatus	Supported	Unsupported	
WorkPerformanceCycleHistory	Unsupported	Unsupported	
WorkPlan	Supported	Supported	
WorkPlanSelectionRule	Supported	Supported	
WorkPlanTemplate	Supported	Supported	
WorkPlanTemplateEntry	Supported	Supported	
WorkRewardFundHistory	Unsupported	Unsupported	
WorkRewardFundTypeHistory	Unsupported	Unsupported	
WorkRewardHistory	Unsupported	Unsupported	
WorkStep	Supported	Supported	
WorkStepStatus	Supported	Supported	
WorkStepTemplate	Supported	Supported	
WorkThanks	Supported	Supported	
WorkThanksShare	Supported	Supported	
WorkType	Supported	Supported	
WorkTypeChangeEvent	Unsupported	Unsupported	
WorkTypeFeed	Supported	Unsupported	
WorkTypeHistory	Unsupported	Unsupported	
WorkTypeShare	Supported	Supported	
WorkTypeGroup	Supported	Supported	
WorkTypeGroupMember	Supported	Supported	

Supported and Unsupported Salesforce Financial Services Cloud Objects

Example

Refer to the following table to view the supported and unsupported Salesforce Financial Services Cloud objects in backup and restore. To learn more details about the objects in the Salesforce Financial Services Cloud platform, see Salesforce Financial Services Cloud object reference.

Object Name	**Support Status in Backup**	**Support Status in Restore**
Account Custom Fields	Supported	Supported
AccountAccountRelation	Supported	Supported
AccountContactRelation	Supported	Supported
AccountParticipant	Supported	Supported
Alert	Supported	Supported
AssetsAndLiabilities	Supported	Supported
AuthFormRequestRecord	Supported	Supported
AuthorizationFormConsent	Supported	Supported
AuthorizationFormText	Supported	Supported
AuthorizedInsuranceLine	Supported	Supported
Award	Supported	Supported
Banker	Supported	Supported
BillingStatement	Supported	Supported
BranchUnit	Supported	Supported
BranchUnitBusinessMember	Supported	Supported
BranchUnitCustomer	Supported	Supported
BranchUnitRelatedRecord	Supported	Supported
BusinessLicense	Supported	Supported
BusinessMilestone	Supported	Supported
BusinessProfile	Supported	Supported
Card	Supported	Supported
CaseGatewayRequest	Supported	Supported
ChargesAndFees	Supported	Supported
Claim	Supported	Supported
ClaimCase	Supported	Supported
ClaimCoverage	Supported	Supported
ClaimCoveragePaymentDetail	Supported	Supported
ClaimCoverageReserveDetail	Supported	Supported
ClaimCovPaymentAdjustment	Supported	Supported
ClaimCovReserveAdjustment	Supported	Supported
ClaimFinancialSettings	Supported	Supported
ClaimItem	Supported	Supported
ClaimParticipant	Supported	Supported
ClaimPaymentSummary	Supported	Supported
ClaimPayoutPlan	Supported	Supported
ClaimRecovery	Supported	Supported
ClaimTeamMember	Supported	Supported
Contact Custom Fields	Supported	Supported
ContactContactRelation	Supported	Supported
ContractGroupPlan	Supported	Supported
ContractGroupPlanGroupClass	Supported	Supported
CoverageType	Supported	Supported

Object Name	Support Status in Backup	Support Status in Restore
CustomerProperty	Supported	Supported
DataUsePurpose	Supported	Supported
DistributorAuthorization	Supported	Supported
DocumentChecklistItem	Supported	Unsupported
DocumentType	Supported	Supported
Education	Supported	Supported
Employment	Supported	Supported
Event Custom Fields	Supported	Supported
FinancialAccount	Supported	Supported
FinancialAccountRole	Supported	Supported
FinancialAccountTransaction	Supported	Supported
FinancialDeal	Supported	Supported
FinancialDealAsset	Supported	Supported
FinancialDealBid	Supported	Supported
FinancialDealInteraction	Supported	Supported
FinancialDealParticipant	Supported	Supported
FinancialDealParty	Supported	Supported
FinancialDealProduct	Supported	Supported
FinancialGoal	Supported	Supported
FinancialHolding	Supported	Supported
FinclDealInteractionSummary	Supported	Supported
FinServ__IndustriesAppConfig__c	Supported	Supported
FinServ__IndustriesSettings__c	Supported	Supported
FinServ__NextLastInteractionSettings__c	Supported	Supported
FinServ__RollupByLookupConfig__c	Supported	Supported
FinServ__RollupByLookupFilterCriteria__c	Supported	Supported
FinServ__UsePersonAccount__c	Supported	Supported
GroupCensus	Supported	Supported
GroupCensusMember	Supported	Supported
GroupCensusMemberPlan	Supported	Supported
GroupClass	Supported	Supported
GroupClassContribution	Supported	Supported
IdentificationDocument	Supported	Supported
IdentityDocument	Supported	Supported
InfoAuthorizationRequest	Supported	Supported
InfoAuthRequestForm	Supported	Supported
InsPolicyTransactionDetail	Supported	Supported
InsuranceClaimAsset	Supported	Supported
InsuranceContract	Supported	Supported
InsurancePolicy	Supported	Supported

Object Name	**Support Status in Backup**	**Support Status in Restore**
InsurancePolicyAsset	Supported	Supported
InsurancePolicyCoverage	Supported	Supported
InsurancePolicyMemberAsset	Supported	Supported
InsurancePolicyParticipant	Supported	Supported
InsurancePolicySurcharge	Supported	Supported
InsurancePolicyTransaction	Supported	Supported
InsuranceProfile	Supported	Supported
Interaction	Supported	Supported
InteractionAttendee	Supported	Supported
InteractionParticipant	Supported	Supported
InteractionRelatedAccount	Supported	Supported
InteractionSumDiscussedAccount	Supported	Supported
InteractionSummary	Supported	Supported
InteractionSummaryParticipant	Supported	Supported
Lead Custom Fields	Supported	Supported
LifeEvent	Supported	Supported
LoanApplicant	Supported	Supported
LoanApplicantAddress	Supported	Supported
LoanApplicantAsset	Supported	Supported
LoanApplicantDeclaration	Supported	Supported
LoanApplicantEmployment	Supported	Supported
LoanApplicantIncome	Supported	Supported
LoanApplicantLiability	Supported	Supported
LoanApplicationFinancial	Supported	Supported
LoanApplicationProperty	Supported	Supported
LoanApplicationTitleHolder	Supported	Supported
MultipartyInfoAuthRequest	Supported	Supported
Opportunity Custom Fields	Supported	Supported
OpportunityParticipant	Supported	Supported
ParticipantRole	Supported	Supported
PartyCertifiedCapacity	Supported	Supported
PartyIdentityVerification	Supported	Supported
PartyIdentityVerificationStep	Supported	Supported
PartyIncome	Unsupported	Unsupported
PartyProfile	Supported	Supported
PartyProfileAddress	Supported	Supported
PartyProfileRisk	Supported	Supported
PartyScreeningStep	Supported	Supported
PartyScreeningSummary	Supported	Supported
PaymentRequest	Supported	Supported
PaymentRequestLine	Supported	Supported
PersonEducation	Supported	Supported

Object Name	Support Status in Backup	Support Status in Restore
PersonLifeEvent	Supported	Supported
PolicyPaymentMethod	Supported	Supported
Producer	Supported	Supported
ProducerCommission	Supported	Supported
ProducerPolicyAssignment	Supported	Supported
ProductCoverage	Supported	Supported
RecAlrtDataSrcExpSetDef	Unsupported	Unsupported
ReciprocalRole	Supported	Supported
RecordAlert	Supported	Supported
RecordAlertDataSource	Supported	Unsupported
RecordAlertDataTranslation	Supported	Supported
RecordAlertTemplate	Supported	Supported
ResidentialLoanApplication	Supported	Supported
Revenue	Supported	Supported
Securities	Supported	Supported
SecuritiesHolding	Supported	Supported
TagCategory	Supported	Supported
Task Custom Fields	Supported	Supported
User Custom Fields	Supported	Supported
UserFinancialAuthority	Supported	Supported
WealthAppConfig	Supported	Supported
WorkerCompCoverageClass	Supported	Supported

Appendix C - Exported Profile Names for Built-in Salesforce Profiles

The table below shows the profile names for several built-in Salesforce profiles and their associated exported profile names. To avoid overwriting these built-in Salesforce profiles, do not name a custom profile the same name as any of these exported profile names.

> **Note:** Profile names that are not listed in this table use the same profile name when they are exported.

Profile Names	Exported Profile Names
System Administrator	Admin
Standard User	Standard
Marketing User	MarketingProfile
Contract Manager	ContractManager
Solution Manager	SolutionManager
Read Only	ReadOnly
Customer Portal Manager	CustomerManager
Customer Portal User	CustomerUser
High Volume Customer Portal	HighVolumePortal
Partner User	Partner
Authenticated Website	PlatformPortal

Profile Names	Exported Profile Names
Standard Platform User	StandardAul

Appendix D - IBM® Storage Protect for Cloud Salesforce Subscription Retention Information

IBM® Storage Protect for Cloud Salesforce provides the following subscription options:

- The **Trial** subscription provides a maximum of six backup jobs per day, including both scheduled and manual backup jobs (four scheduled backup jobs at most). It also includes the backup of a sandbox organization, as well as the restore and the compare features. After the subscription is expired, IBM® Storage Protect for Cloud Salesforce will keep the backup data for 30 days. If you do not purchase a subscription, the data will be deleted. Before the data is deleted, you can contact IBM Software Support team to retrieve the backup data.

- The **Enterprise** subscription provides a maximum of eight backup jobs per day, including both scheduled and manual backup jobs (four scheduled backup jobs at most). It also includes the backup of a sandbox organization, as well as the restore and the compare features. With this subscription, you can restore all of the backup data. After the subscription expires, IBM® Storage Protect for Cloud Salesforce will keep the backup data for 60 days. If you do not extend the subscription or purchase an additional subscription, the data will be deleted. Before the data is deleted, you can contact IBM Software Support team to retrieve the backup data.

Appendix E - Supported and Unsupported Fields in Data Anonymization and Cleanup

Refer to the following table to view the supported and unsupported fields in data anonymization and cleanup.

Field	Support Status in Data Anonymization	Support Status in Data Cleanup
Address	Supported	Supported
Auto Number	Unsupported	Unsupported
Checkbox	Supported	Unsupported
Currency	Supported	Supported
Date	Supported	Supported
Date/Time	Supported	Supported
Email	Supported	Supported
External Lookup Relationship	Unsupported	Unsupported
Formula	Unsupported	Unsupported
Geolocation	Supported	Supported
Hierarchical Relationship	Unsupported	Unsupported
Indirect Lookup Relationship	Unsupported	Unsupported
Lookup Relationship	Unsupported	Unsupported
Master-Detail Relationship	Unsupported	Unsupported
Number	Supported	Supported
Percent	Supported	Supported
Phone	Supported	Supported
Picklist	Unsupported	Unsupported
Picklist (Multi-select)	Unsupported	Unsupported
Roll-Up Summary	Unsupported	Unsupported
Text	Supported	Supported

Field	Support Status in Data Anonymization	Support Status in Data Cleanup
Text (Encrypted)	Supported	Supported
Text Area	Supported	Supported
Text Area (Long)	Supported	Supported
Text Area (Rich)	Supported	Supported
Time	Supported	Supported
URL	Supported	Supported

Appendix F - Supported and Unsupported Metadata Types for Backup and Restore

Refer to the following table to view the supported and unsupported metadata types in backup and restore. To learn more details about the Salesforce objects, see Salesforce metadate types reference.

Object Name	Support Status in Backup	Support Status in Restore
AccountRelationshipShareRule	Supported	Unsupported
ActionLinkGroupTemplate	Supported	Unsupported
ActionPlanTemplate	Supported	Unsupported
AdvAccountForecastSet	Supported	Unsupported
AnalyticSnapshot	Supported	Unsupported
ApexClass	Supported	Supported
ApexComponent	Supported	Unsupported
ApexPage	Supported	Unsupported
ApexTestSuite	Supported	Unsupported
ApexTrigger	Supported	Supported
ApprovalProcess	Supported	Supported
AssignmentRules	Supported	Supported
Audience	Supported	Unsupported
AuraDefinitionBundle	Supported	Unsupported
AuthProvider	Supported	Unsupported
AutoResponseRules	Supported	Unsupported
BriefcaseDefinition	Supported	Unsupported
CampaignInfluenceModel	Supported	Unsupported
Certificate	Supported	Unsupported
Community (Zone)	Supported	Unsupported
ConnectedApp	Supported	Unsupported
ContentAsset	Supported	Unsupported
ContentAsset	Supported	Unsupported
CorsWhitelistOrigin	Supported	Unsupported
CspTrustedSite	Supported	Unsupported
CustomApplication	Supported	Unsupported
CustomApplicationComponent	Supported	Unsupported
CustomFeedFilter	Supported	Unsupported
CustomHelpMenuSection	Supported	Unsupported

Object Name	Support Status in Backup	Support Status in Restore
CustomLabels	Supported	Supported
Custom Metadata Types (CustomObject)	Supported	Unsupported
CustomNotificationType	Supported	Unsupported
CustomObject	Supported	Supported
CustomObjectTranslation	Supported	Unsupported
CustomPageWebLink	Supported	Unsupported
CustomPermission	Supported	Unsupported
CustomSite	Supported	Unsupported
CustomTab	Supported	Unsupported
CustomValue	Supported	Unsupported
Dashboard	Supported	Supported
DataCategoryGroup	Supported	Unsupported
DecisionTable	Supported	Unsupported
DecisionTableDatasetLink	Supported	Unsupported
DelegateGroup	Supported	Unsupported
DigitalExperienceBundle	Supported	Unsupported
DigitalExperienceConfig	Supported	Unsupported
DisclosureDefinition	Supported	Unsupported
DisclosureDefinitionVersion	Supported	Unsupported
DisclosureType	Supported	Unsupported
DiscoveryAIModel	Supported	Unsupported
DiscoveryGoal	Supported	Unsupported
Document	Unsupported	Unsupported
DocumentChecklistSettings	Supported	Unsupported
DocumentType	Supported	Unsupported
DuplicateRule	Supported	Unsupported
EmailServicesFunction	Supported	Unsupported
EmailTemplate	Supported	Supported
EmbeddedServiceConfig	Supported	Unsupported
EmbeddedServiceMenuSettings	Supported	Unsupported
EntitlementProcess	Supported	Unsupported
EntitlementTemplate	Supported	Unsupported
EscalationRules	Supported	Unsupported
ExperienceBundle	Supported	Unsupported
ExplainabilityMsgTemplate	Supported	Unsupported
ExpressionSetDefinition	Supported	Unsupported
ExpressionSetMessageToken	Supported	Unsupported
ExpressionSetObjectAlias	Supported	Unsupported
ExternalAuthIdentityProvider	Supported	Unsupported
ExternalClientApplication	Supported	Unsupported
ExternalCredential	Supported	Unsupported

Object Name	Support Status in Backup	Support Status in Restore
ExternalServiceRegistration	Supported	Unsupported
ExtlClntAppConfigurablePolicies	Supported	Unsupported
ExtlClntAppGlobalOauthSettings	Supported	Unsupported
ExtlClntAppOauthConfigurablePolicies	Supported	Unsupported
ExtlClntAppOauthSettings	Supported	Unsupported
ExtlClntAppSamlConfigurablePolicies	Supported	Unsupported
FieldRestrictionRule	Supported	Unsupported
FlexiPage	Supported	Supported
Flow	Supported	Supported
FlowCategory	Supported	Unsupported
FlowDefinition	Supported	Unsupported
Folder	Supported	Supported
ForecastingSourceDefinition	Supported	Unsupported
ForecastingType	Supported	Unsupported
ForecastingTypeSource	Supported	Unsupported
GatewayProviderPaymentMethodType	Supported	Unsupported
GlobalPicklist	Supported	Supported
GlobalPicklistValue	Supported	Supported
GlobalValueSet	Supported	Supported
GlobalValueSetTranslation	Supported	Unsupported
Group	Supported	Unsupported
HomePageComponent	Supported	Unsupported
HomePageLayout	Supported	Unsupported
IdentityVerificationProcDef	Supported	Unsupported
InboundCertificate	Supported	Unsupported
InstalledPackage	Supported	Unsupported
Layout	Supported	Supported
Letterhead	Supported	Unsupported
LightningMessageChannel	Supported	Unsupported
LightningOnboardingConfig	Supported	Unsupported
ManagedContentType	Supported	Unsupported
ManagedTopics	Supported	Unsupported
MatchingRule	Supported	Unsupported
Metadata	Supported	Supported
MilestoneType	Supported	Unsupported
ModerationRule	Supported	Unsupported
MutingPermissionSet	Supported	Supported
NamedCredential	Supported	Unsupported
NavigationMenu	Supported	Unsupported
Network	Supported	Unsupported

Object Name	Support Status in Backup	Support Status in Restore
NetworkBranding	Supported	Unsupported
NotificationTypeConfig	Supported	Supported
OmniScript	Supported	Unsupported
OmniSupervisorConfig	Unsupported	Unsupported
OutboundNetworkConnection	Supported	Unsupported
Package	Supported	Unsupported
ParticipantRole	Supported	Unsupported
PathAssistant	Supported	Unsupported
PermissionSet	Supported	Supported
PermissionSetGroup	Supported	Supported
PersonAccountOwnerPowerUser	Supported	Unsupported
PlatformCachePartition	Supported	Unsupported
PlatformEventChannelMember	Supported	Unsupported
Portal	Supported	Unsupported
PortalDelegablePermissionSet	Supported	Unsupported
PresenceDeclineReason	Supported	Unsupported
PresenceUserConfig	Supported	Unsupported
Profile	Supported	Supported
ProfilePasswordPolicy	Supported	Unsupported
ProfileSessionSetting	Supported	Unsupported
Prompt	Supported	Unsupported
Queue	Supported	Unsupported
QueueRoutingConfig	Supported	Unsupported
QuickAction	Supported	Supported
RedirectWhitelistUrl	Supported	Unsupported
RecordActionDeployment	Supported	Unsupported
RecordAggregationDefinition	Supported	Unsupported
RelationshipGraphDefinition	Supported	Unsupported
RemoteSiteSetting	Supported	Unsupported
Report	Supported	Supported
ReportType	Supported	Supported
RestrictionRule	Unsupported	Unsupported
Role	Supported	Unsupported
ServiceChannel	Supported	Unsupported
ServicePresenceStatus	Supported	Unsupported
Settings	Supported	Unsupported
SharingRules	Supported	Supported
StandardValueSetTranslation	Supported	Unsupported
StaticResource	Supported	Unsupported
Territory2Model	Supported	Unsupported
Territory2Rule	Supported	Unsupported
Territory2Type	Supported	Unsupported

Object Name	Support Status in Backup	Support Status in Restore
TopicsForObjects	Supported	Unsupported
TransactionSecurityPolicy	Supported	Unsupported
Translations	Supported	Unsupported
UserCriteria	Supported	Unsupported
WaveAnalyticAssetCollection	Supported	Unsupported
WaveApplication	Supported	Unsupported
WaveDataflow	Supported	Unsupported
WaveDashboard	Supported	Unsupported
WaveDataset	Supported	Unsupported
WaveRecipe	Supported	Unsupported
WebStoreBundle	Unsupported	Unsupported
Workflow	Supported	Supported
WorkSkillRouting	Supported	Unsupported

Notices

This information was developed for products and services offered in the US. This material might be available from IBM® in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM® representative for information on the products and services currently available in your area. Any reference to an IBM® product, program, or service is not intended to state or imply that only that IBM® product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM® intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM® product, program, or service.

IBM® may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM® Intellectual Property Department in your country or send inquiries, in writing, to:
Intellectual Property Licensing
Legal and Intellectual Property Law
IBM® Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM® may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM® websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM® product and use of those websites is at your own risk.

IBM® may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM® under terms of the IBM® Customer Agreement, IBM® International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM® products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM® has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM® products. Questions on the capabilities of non-IBM® products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

IBM®, the IBM® logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM® or other companies. A current list of IBM® trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe™ is a registered trademark of Adobe™ Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open™, LTO™, and Ultrium™ are trademarks of HP, IBM® Corp. and Quantum in the U.S. and other countries.

Intel™ and Itanium™ are trademarks or registered trademarks of Intel™ Corporation or its subsidiaries in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from the Linux® Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft™, Windows™, and Windows NT™ are trademarks of Microsoft™ Corporation in the United States, other countries, or both.

Java™ and all Java™-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Red Hat®, OpenShift®, Ansible®, and Ceph® are trademarks or registered trademarks of Red Hat®, Inc. or its subsidiaries in the United States and other countries.

UNIX® is a registered trademark of The Open Group in the United States and other countries.

VMware, VMware vCenter Server™, and VMware vSphere™ are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM® website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM®.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM®.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.
IBM® reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM®, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM® MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM® Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM®'s Privacy Policy at http://www.ibm.com/privacy and IBM®'s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM® Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.